

## Active Information Gathering & Web Traffic Analysis

Target: OWASP Juice Shop

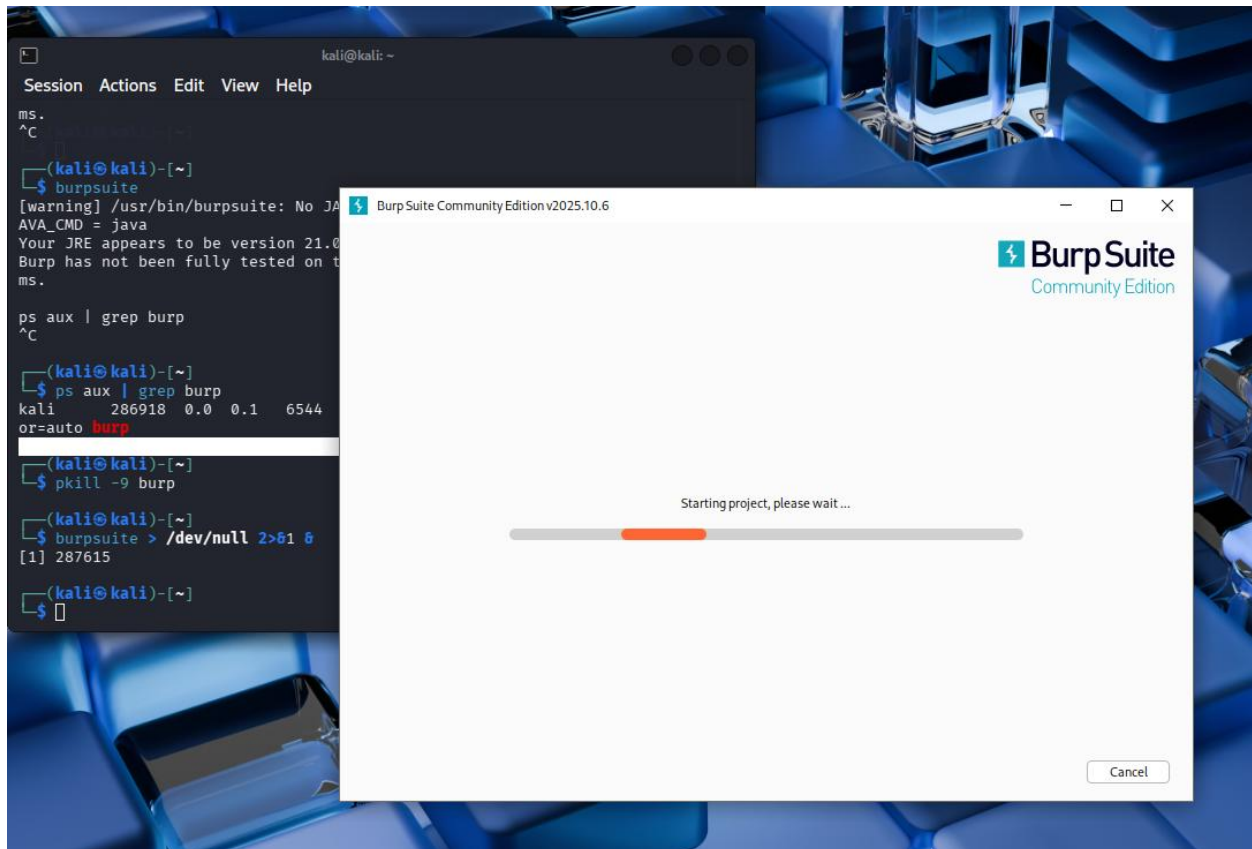
URL: <https://demo.owasp-juice.shop>

Reason for Selection:

OWASP Juice Shop is an intentionally vulnerable web application designed for legal security testing and learning purposes.

**Burp Suite was launched from the Kali Linux terminal to ensure proper integration with the system and browser traffic interception.**

```
(kali@kali)-[~]
$ burpsuite
[warning] /usr/bin/burpsuite: No JAVA_CMD set for run_java, falling back to J
AVA_CMD = java
Your JRE appears to be version 21.0.9 from Debian
Burp has not been fully tested on this platform and you may experience proble
ms.
```



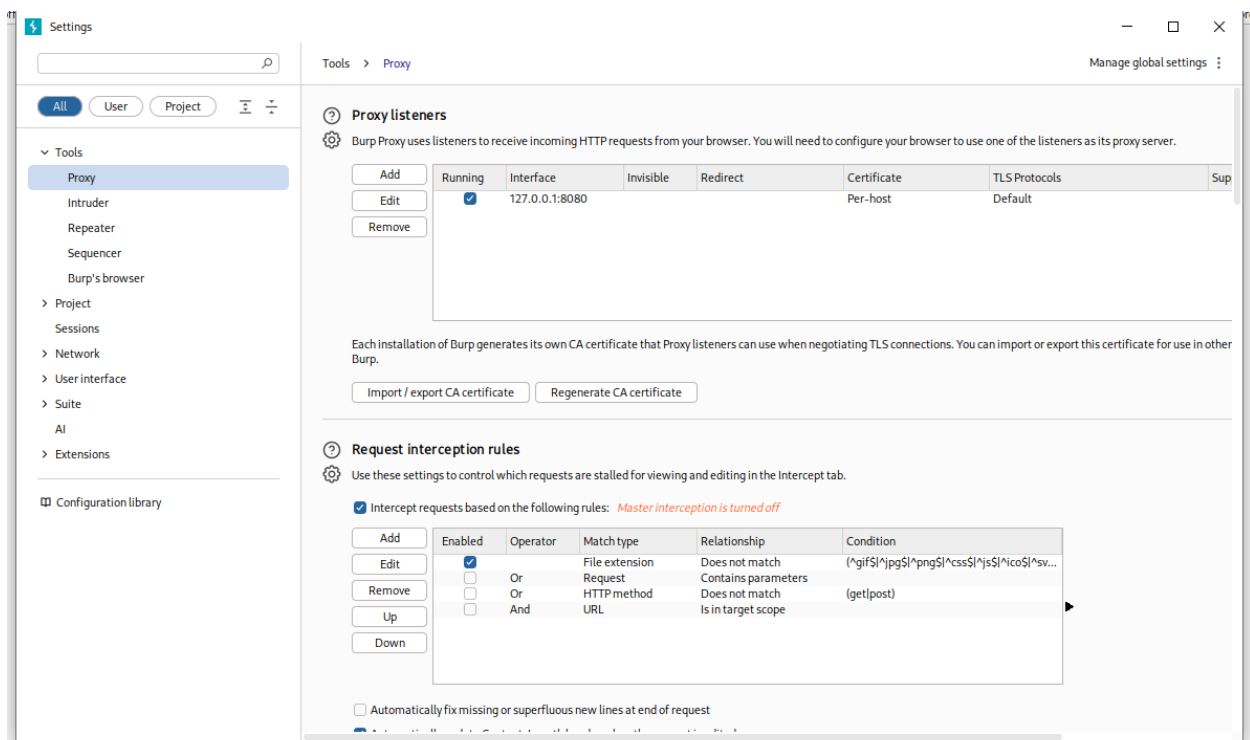


Figure 1 Burp proxy listener active on localhost (127.0.0.1) port 8080, ready to capture traffic from Firefox browser.

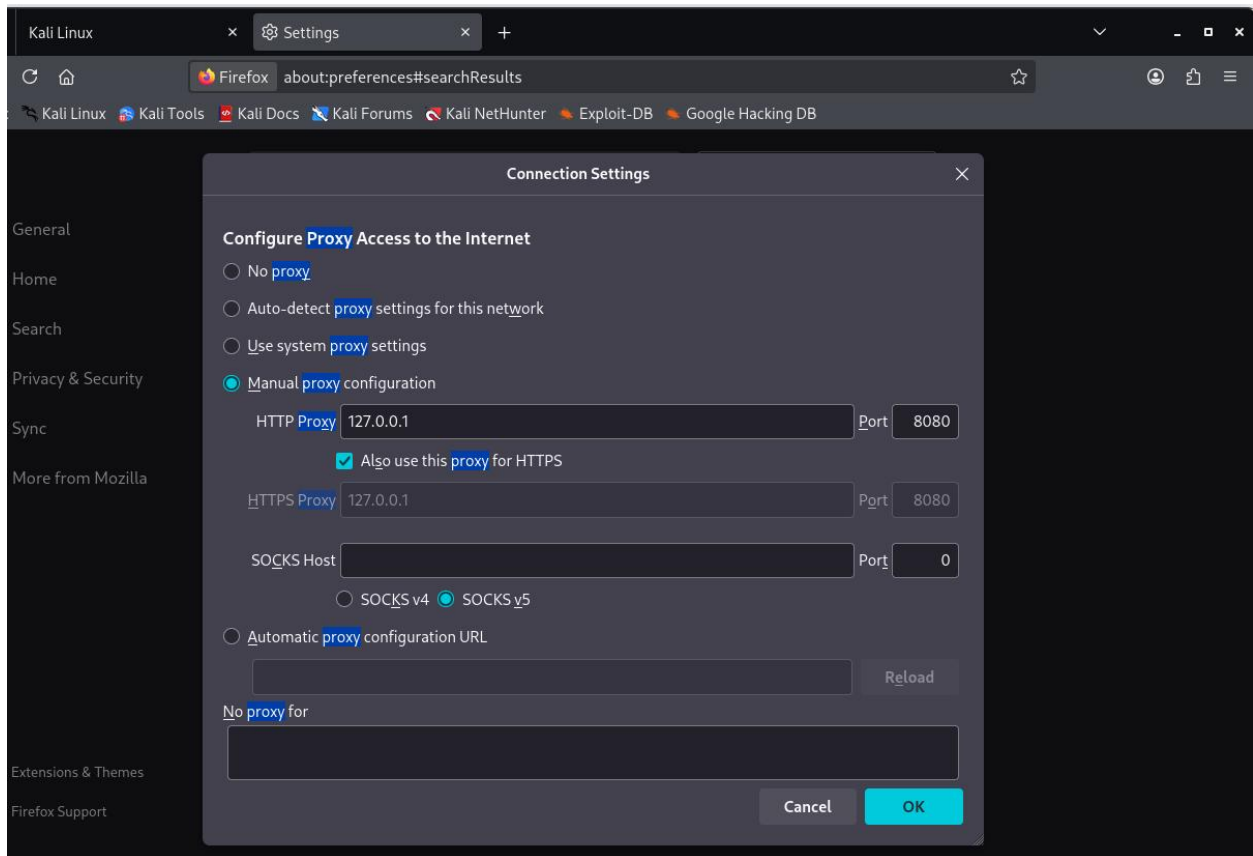


Figure 2 firefox\_proxy\_settings.png

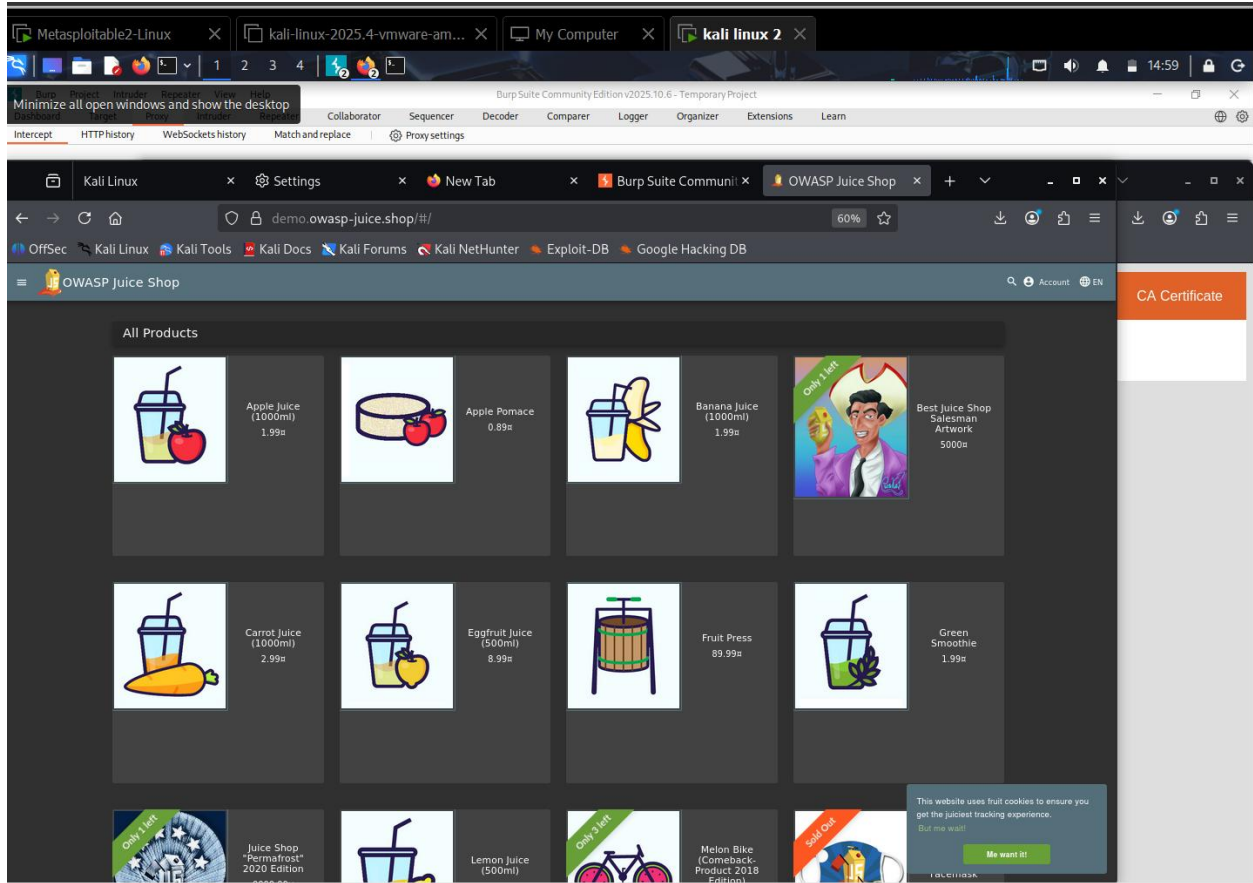


Figure 3 The OWASP Juice Shop website loading properly

1 2 3 4

Burp Suite Community Edition v2025.10.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP History WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS and image content; hiding specific extensions Filter on

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	Start respon
1	https://demo.owasp-juice.s...	GET	/			200	76007	HTML		OWASP Juice Shop		12498
2	https://demo.owasp-juice.s...	GET	/			200	76007	HTML		OWASP Juice Shop		9236
9	https://demo.owasp-juice.s...	GET	/assets/i18n/en.json			503	1309	HTML	json	Application Error		4349
10	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...			503	1309	HTML	io/	Application Error		4332
11	https://demo.owasp-juice.s...	GET	/rest/admin/application-configura...			503	1309	HTML		Application Error		4346
12	https://demo.owasp-juice.s...	GET	/rest/admin/application-version			503	1309	HTML		Application Error		4342
13	https://demo.owasp-juice.s...	GET	/rest/languages			503	1289	HTML		Application Error		8449
14	https://demo.owasp-juice.s...	GET	/api/Challenges/?name=Score%2...			503	1289	HTML		Application Error		8396
15	https://demo.owasp-juice.s...	GET	/rest/admin/application-version			503	1309	HTML		Application Error		4325
16	https://demo.owasp-juice.s...	GET	/api/Challenges/?name=Score%2...			503	1289	HTML		Application Error		8376
17	https://demo.owasp-juice.s...	GET	/rest/admin/application-configura...			503	1289	HTML		Application Error		8390
18	https://demo.owasp-juice.s...	GET	/rest/admin/application-configura...			503	1309	HTML		Application Error		4326

Toggle your filter on or off  
Quickly compare filtered and unfiltered traffic without resetting your filter.  
Learn more Got it

1 2 3 4

Burp Suite Community Edition v2025.10.6 - Temporary Project

Applications Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP History WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS and image content; hiding specific extensions Filter on

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	Start respon
123	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...			200	740	text	io/			254
124	https://demo.owasp-juice.s...	POST	/socket.io/?EIO=4&transport=polli...			200	721	HTML	io/			415
125	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...			200	736	text	io/			255
126	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...			200	744	text	io/			254
127	https://demo.owasp-juice.s...	POST	/socket.io/?EIO=4&transport=polli...			200	729	HTML	io/			487
128	https://demo.owasp-juice.s...	POST	/socket.io/?EIO=4&transport=polli...			200	721	HTML	io/			384
129	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...			200	736	text	io/			253
130	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...			200	827	text	io/			119
131	https://demo.owasp-juice.s...	POST	/socket.io/?EIO=4&transport=polli...			200	717	HTML	io/			482
132	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...			200	740	text	io/			135
133	https://demo.owasp-juice.s...	POST	/socket.io/?EIO=4&transport=polli...			200	725	HTML	io/			452
134	https://demo.owasp-juice.s...	POST	/socket.io/?EIO=4&transport=polli...			200	827	text	io/			176

Toggle your filter on or off  
Quickly compare filtered and unfiltered traffic without resetting your filter.  
Learn more Got it

## Request

Pretty Raw Hex

```
1 POST /socket.io/?EIO=4&transport=polling&t=PmGVDSb&sid=
2 RyZgXgyUoSJcYwZ9ACUN HTTP/2
3 Host: demo.owasp-juice.shop
4 Cookie: language=en; welcomebanner_status=dismiss
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101
6 Firefox/140.0
7 Accept: */*
8 Accept-Language: en-US,en;q=0.5
9 Accept-Encoding: gzip, deflate, br
10 Content-Type: text/plain; charset=UTF-8
11 Content-Length: 1
12 Origin: https://demo.owasp-juice.shop
13 Referer: https://demo.owasp-juice.shop/
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17 Te: trailers
18
```

## Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Access-Control-Allow-Origin: http://localhost:4200
3 Content-Length: 2
4 Content-Type: text/html
5 Date: Fri, 30 Jan 2026 19:59:01 GMT
6 Nel:
7 {"report_to":"heroku-nel","response_headers":["Via"],"max_age":3600,"succe
8 ss_fraction":0.01,"failure_fraction":0.1}
9 Report-To:
10 {"group":"heroku-nel","endpoints":[{"url":"https://nel.heroku.com/reports?
11 s=0LrawFXDuqOp%2FPMgwOrp1PomcGhFEcRaycMnxA7kE%3D%u0026sid=812dccc77-0bd0-
12 43b1-a5f1-b25750382959%u0026ts=1769803141"}],"max_age":3600}
13 Reporting-Endpoints:
14 heroku-nel="https://nel.heroku.com/reports?s=0LrawFXDuqOp%2FPMgwOrp1Pomc
15 GhFEcRaycMnxA7kE%3D%u0026sid=812dccc77-0bd0-43b1-a5f1-b25750382959&ts=1769803141"
16
17 Server: Heroku
18 Vary: Origin
19 Via: 1.1 heroku-router
20
21 ok
```

## Inspector

Request attributes	2
Request query parameters	4
Request body parameters	1
Request cookies	2
Request headers	18
Response headers	10

1 Burp Project Intruder Repeater View Help Burp Suite Community Edition v2025.10.6 - Temporary Project

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS and image content; hiding specific extensions Filter on

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start respon.
223	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...		✓	200	740	text	io/			✓	81.169.145.156		14:58:36 30 ...	8080	25409
224	https://demo.owasp-juice.s...	POST	/socket.io/?EIO=4&transport=polli...		✓	200	721	HTML	io/			✓	81.169.145.156		14:59:01 30 ...	8080	415
225	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...		✓	200	736	text	io/			✓	81.169.145.156		14:59:01 30 ...	8080	25516
226	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...		✓	200	744	text	io/			✓	81.169.145.156		14:59:27 30 ...	8080	25487
227	https://demo.owasp-juice.s...	POST	/socket.io/?EIO=4&transport=polli...		✓	200	729	HTML	io/			✓	81.169.145.156		14:59:27 30 ...	8080	487
228	https://demo.owasp-juice.s...	POST	/socket.io/?EIO=4&transport=polli...		✓	200	721	HTML	io/			✓	81.169.145.156		14:59:52 30 ...	8080	384
229	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...		✓	200	736	text	io/			✓	81.169.145.156		14:59:52 30 ...	8080	25380
230	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...		✓	200	827	text	io/			✓	81.169.145.156		15:00:18 30 ...	8080	11940
231	https://demo.owasp-juice.s...	POST	/socket.io/?EIO=4&transport=polli...		✓	200	717	HTML	io/			✓	81.169.145.156		15:00:18 30 ...	8080	482
232	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...		✓	200	740	text	io/			✓	81.169.145.156		15:00:30 30 ...	8080	13588
233	https://demo.owasp-juice.s...	POST	/socket.io/?EIO=4&transport=polli...		✓	200	725	HTML	io/			✓	81.169.145.156		15:00:43 30 ...	8080	452
234	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...		✓	200	827	text	io/			✓	81.169.145.156		15:00:43 30 ...	8080	1768

**Request**

Pretty Raw Hex

```
1 GET /socket.io/?EIO=4&transport=polling&token=PmGVDSf6&sid=
2 RyZgXgyUo5JcYwZ9ACUN HTTP/2
3 Host: demo.owasp-juice.shop
4 Cookie: language=en; welcomebanner_status=dismiss
5 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101
6 Firefox/140.0
7 Accept: */*
8 Accept-Language: en-US,en;q=0.5
9 Accept-Encoding: gzip, deflate, br
10 Referer: https://demo.owasp-juice.shop/
11 Sec-Fetch-Dest: empty
12 Sec-Fetch-Mode: cors
13 Te: trailers
14
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Access-Control-Allow-Origin: http://localhost:4200
3 Content-Length: 1
4 Content-Type: text/plain; charset=UTF-8
5 Date: Fri, 30 Jan 2026 19:59:26 GMT
6 Nel:
7 {"report_to":"heroku-nel","endpoints":[{"url":"https://nel.heroku.com/reports?
8 s=0LrawFXDuquOp%2FPMgwOrp1PomcGhFEcraycMnxA7kE%3Du0026sid=812dcc77-0bd0-
9 43b1-a5f1-b25750382959%u0026ts=1769803141"}],"max_age":3600}
10 Server: Heroku
11 Vary: Origin
12 Via: 1.1 heroku-router
13
14 2
```

**Inspector**

Request attributes 2

Request query parameters 4

Request cookies 2

Request headers 15

Response headers 10

Figure 4 GET SS





Dashboard	Target	Proxy	Intruder	Repeater	Collaborator	Sequencer	Decoder	Comparer	Logger	Organizer	Extensions	Learn			
Intercept	HTTP history	WebSockets history	Match and replace		Proxy settings										
Filter settings: Hiding CSS and image content; hiding specific extensions															
#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
1022	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	732	text	io/			✓	81.169.145.156		15:46:37 30 ...
1024	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	736	text	io/			✓	81.169.145.156		15:46:46 30 ...
1026	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	740	text	io/			✓	81.169.145.156		15:47:02 30 ...
1027	https://demo.owasp-juice.s...	GET	/rest/user/whoami			304	810					✓	81.169.145.156		15:47:10 30 ...
1028	https://demo.owasp-juice.s...	GET	/rest/products/42/reviews			200	1279	JSON				✓	81.169.145.156		15:47:10 30 ...
1029	https://demo.owasp-juice.s...	GET	/rest/products/42/reviews			200	1279	JSON				✓	81.169.145.156		15:47:10 30 ...
1030	https://demo.owasp-juice.s...	GET	/rest/products/42/reviews			304	819					✓	81.169.145.156		15:47:11 30 ...
1032	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	736	text	io/			✓	81.169.145.156		15:47:12 30 ...
1034	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	740	text	io/			✓	81.169.145.156		15:47:28 30 ...
1035	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	732	text	io/			✓	81.169.145.156		15:47:37 30 ...
1038	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	732	text	io/			✓	81.169.145.156		15:47:53 30 ...
1040	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	736	text	io/			✓	81.169.145.156		15:48:02 30 ...

[illegible]

Figure 7 session persistence

Filter settings: Hiding CSS and image content; hiding specific extensions														
#	Host	Met...	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies
1022	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	732	text	io/			✓	81.169.145.156	
1024	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	736	text	io/			✓	81.169.145.156	
1026	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	740	text	io/			✓	81.169.145.156	
1027	https://demo.owasp-juice.s...	GET	/rest/user/whoami			304	810					✓	81.169.145.156	
1028	https://demo.owasp-juice.s...	GET	/rest/products/42/reviews			200	1279	JSON				✓	81.169.145.156	
1029	https://demo.owasp-juice.s...	GET	/rest/products/42/reviews			200	1279	JSON				✓	81.169.145.156	
1030	https://demo.owasp-juice.s...	GET	/rest/products/42/reviews			304	819					✓	81.169.145.156	
1032	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	736	text	io/			✓	81.169.145.156	
1034	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	740	text	io/			✓	81.169.145.156	
1035	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	732	text	io/			✓	81.169.145.156	
1038	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	732	text	io/			✓	81.169.145.156	
1040	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	736	text	io/			✓	81.169.145.156	

[illegible]

Figure 8 cookies

Cookie attributes were not explicitly visible in captured responses; however, secure session handling was observed via token-based authentication



#	Host	Met...	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time
003	https://demo.owasp-juice.s...	GET	/api/Challenges/?name=Score%2...	✓		200	1341	JSON				✓	81.169.145.156		15:46
005	https://demo.owasp-juice.s...	GET	/api/Quantity/			304	812					✓	81.169.145.156		15:46
006	https://demo.owasp-juice.s...	GET	/rest/products/search?q=	✓		304	812					✓	81.169.145.156		15:46
008	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	768	text	io/			✓	81.169.145.156		15:46
009	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=web...	✓		400	787	JSON	io/			✓	81.169.145.156		15:46
022	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	732	text	io/			✓	81.169.145.156		15:46
024	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	736	text	io/			✓	81.169.145.156		15:46
026	https://demo.owasp-juice.s...	GET	/socket.io/?EIO=4&transport=polli...	✓		200	740	text	io/			✓	81.169.145.156		15:47
027	https://demo.owasp-juice.s...	GET	/rest/user/whoami			304	810					✓	81.169.145.156		15:47
028	https://demo.owasp-juice.s...	GET	/rest/products/42/reviews			200	1279	JSON				✓	81.169.145.156		15:47
029	https://demo.owasp-juice.s...	GET	/rest/products/42/reviews			200	1279	JSON				✓	81.169.145.156		15:47
030	https://demo.owasp-juice.s...	GET	/rest/products/42/reviews			304	819					✓	81.169.145.156		15:47

Figure 9 few status codes column

## Conclusion

This assignment demonstrated active information gathering and web traffic analysis using **Burp Suite** on the **OWASP Juice Shop** application. HTTP/HTTPS requests and responses were captured to analyze headers, cookies, session tokens, and status codes. Login behavior and session persistence were successfully observed using token-based authentication. The exercise improved practical understanding of web communication and ethical security testing.