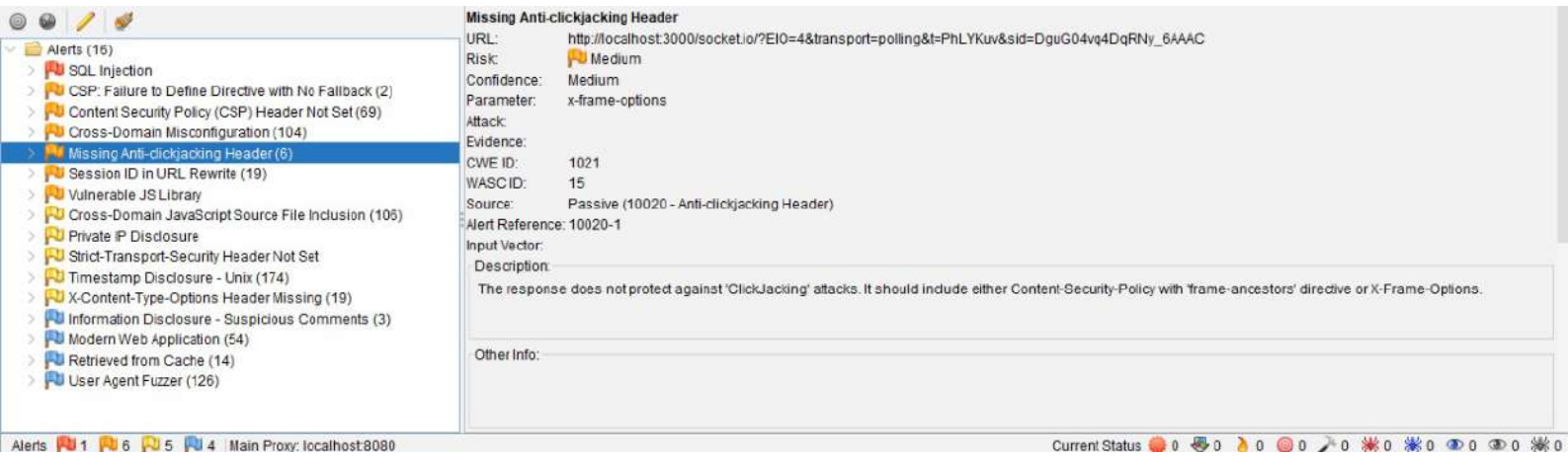
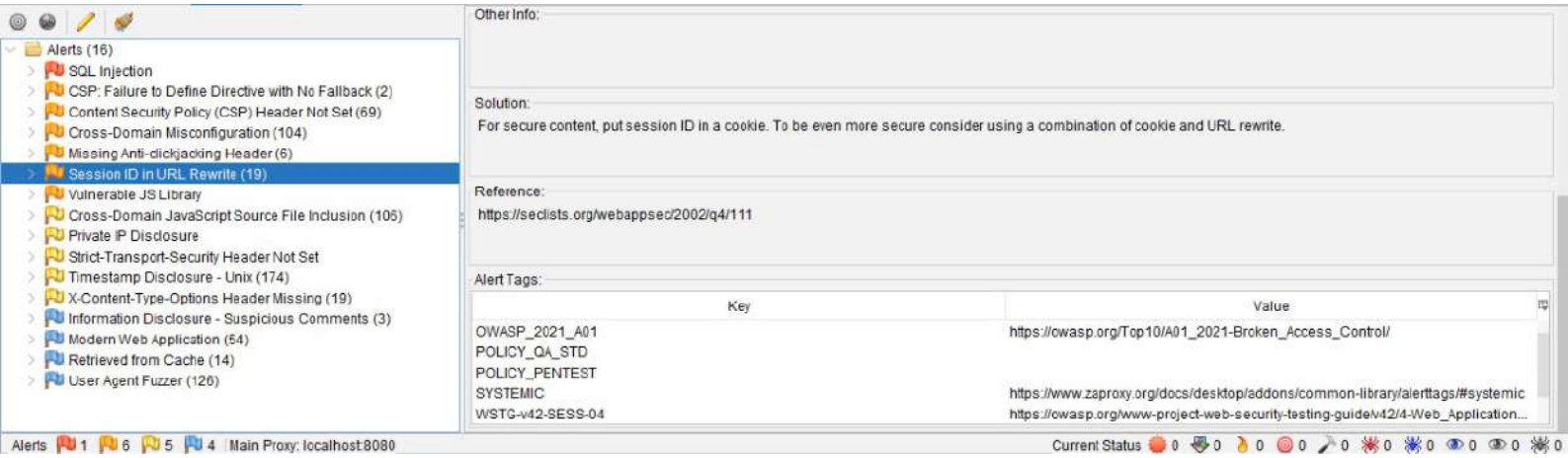
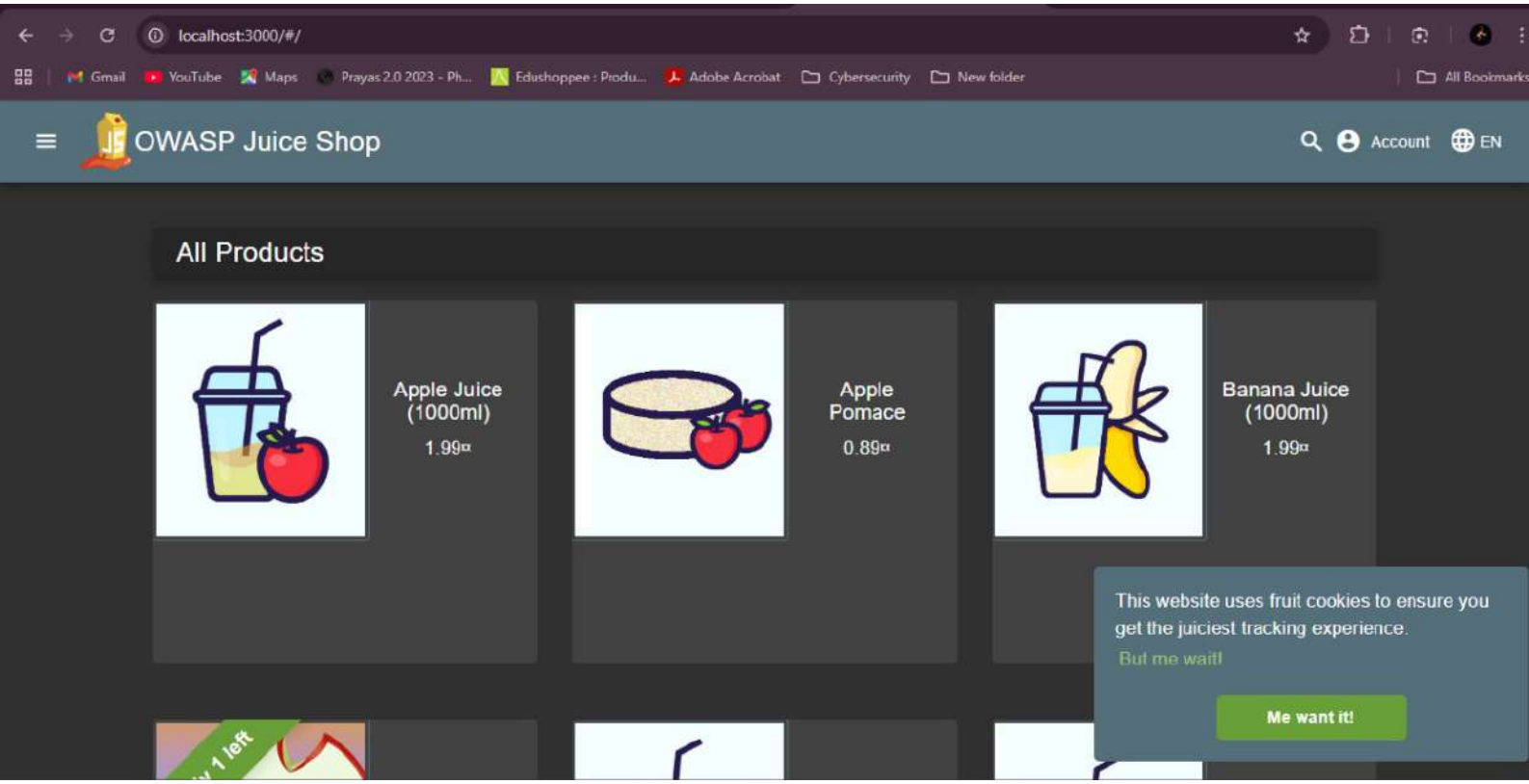
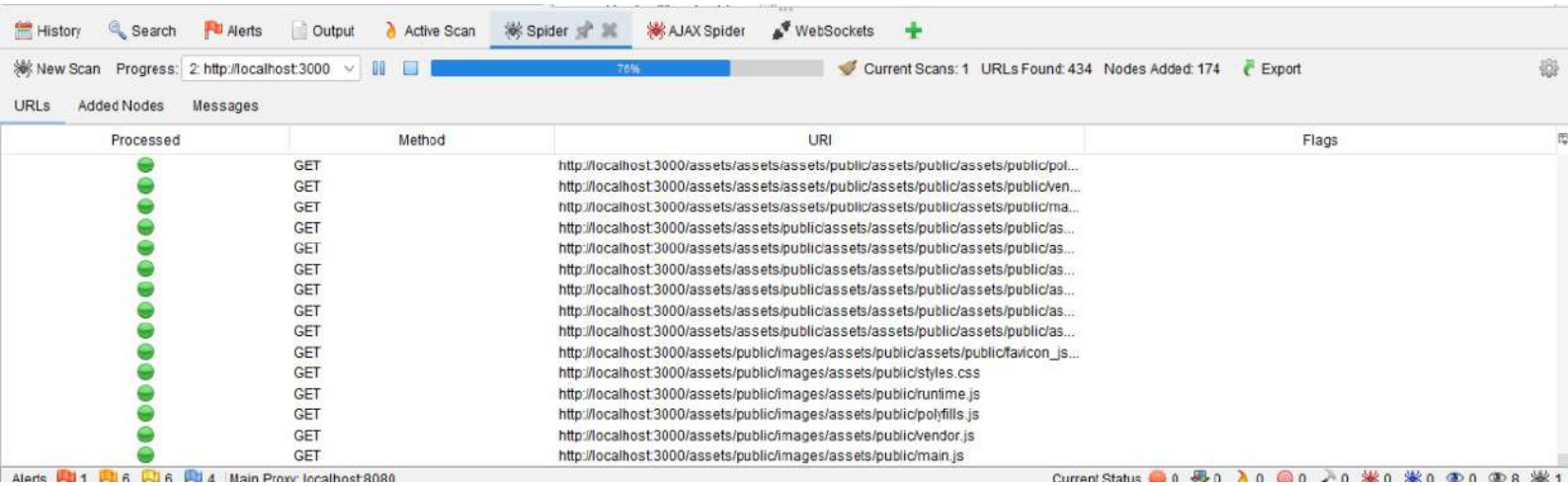

Alerts (16)
SQL Injection
CSP: Failure to Define Directive with No Fallback (2)
Content Security Policy (CSP) Header Not Set (69)
Cross-Domain Misconfiguration (104)
Missing Anti-clickjacking Header (6)
Session ID in URL Rewrite (19)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (105)
Private IP Disclosure
Strict-Transport-Security Header Not Set
Timestamp Disclosure - Unix (174)
X-Content-Type-Options Header Missing (19)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (54)
Retrieved from Cache (14)
User Agent Fuzzer (126)
Missing Anti-clickjacking Header
URL: http://localhost:3000/socket.io/?EIO=4&transport=polling&t=PhLYKuv&sid=DguG04vq4DqRNy_6AAAC
Risk: Medium
Confidence: Medium
Parameter: x-frame-options
Attack:
Evidence:
CWE ID: 1021
WASC ID: 15
Source: Passive (10020 - Anti-clickjacking Header)
Alert Reference: 10020-1
Input Vector:
Description:
The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
Other Info:
Alerts 1 6 5 4 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0

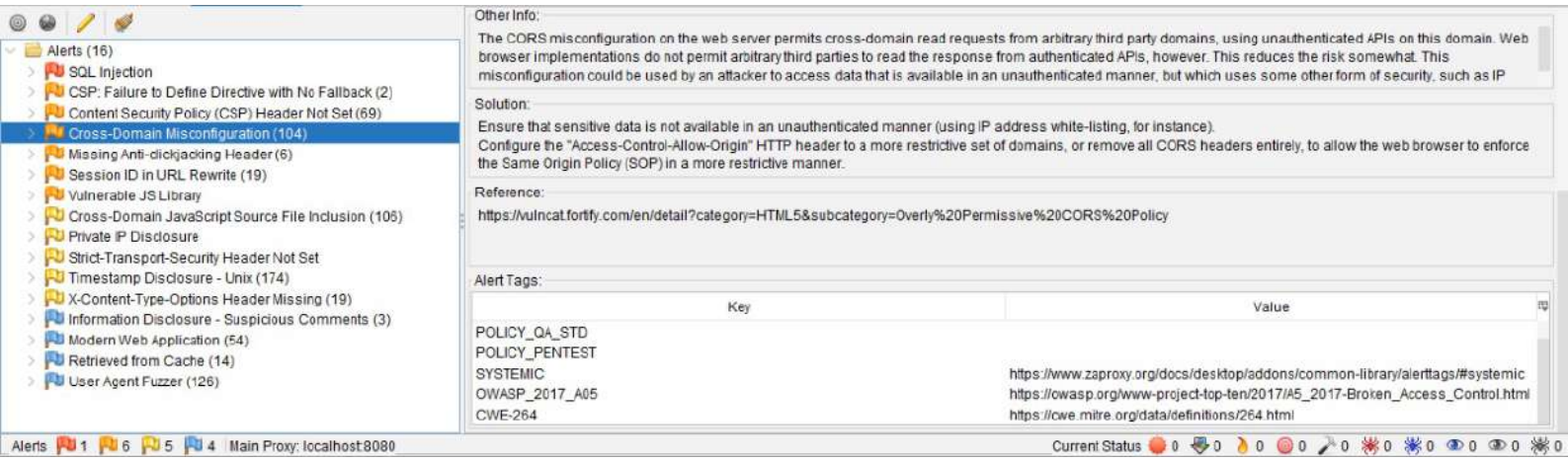

Alerts (16)
SQL Injection
CSP: Failure to Define Directive with No Fallback (2)
Content Security Policy (CSP) Header Not Set (69)
Cross-Domain Misconfiguration (104)
Missing Anti-clickjacking Header (6)
Session ID in URL Rewrite (19)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (105)
Private IP Disclosure
Strict-Transport-Security Header Not Set
Timestamp Disclosure - Unix (174)
X-Content-Type-Options Header Missing (19)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (54)
Retrieved from Cache (14)
User Agent Fuzzer (126)
Other Info:
Solution:
For secure content, put session ID in a cookie. To be even more secure consider using a combination of cookie and URL rewrite.
Reference:
https://seclists.org/webappsec/2002/q4/111
Alert Tags:
Key
Value
OWASP_2021_A01
https://owasp.org/Top10/A01_2021-Broken_Access_Control/
POLICY_QA_STD
POLICY_PENTEST
SYSTEMIC
https://www.zaproxy.org/docs/desktop/addons/common-library/alerttags/#systemic
WSTG-v42-SESS-04
https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application...
Alerts 1 6 5 4
Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0

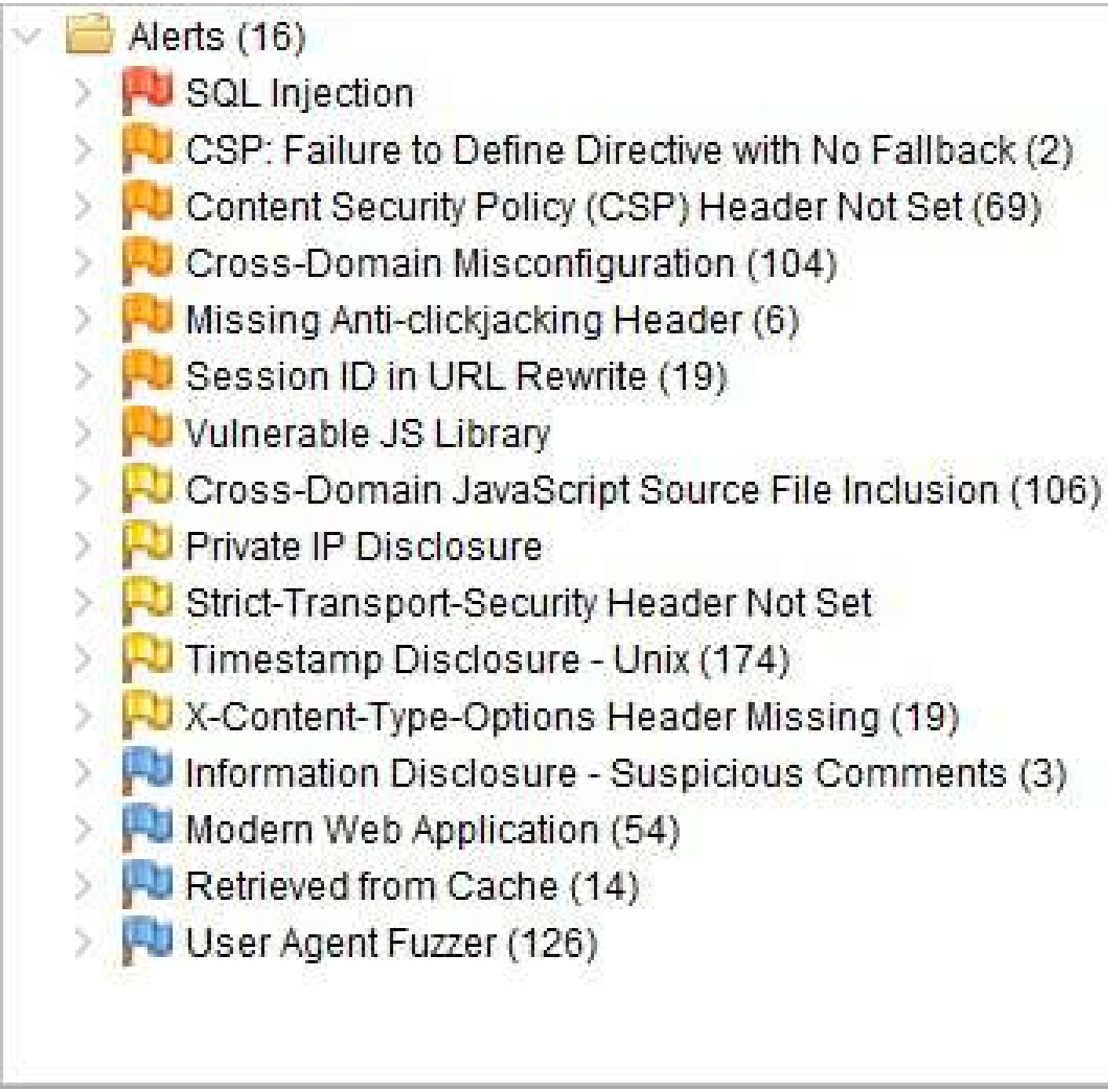

Alerts (16)
SQL Injection
CSP: Failure to Define Directive with No Fallback (2)
Content Security Policy (CSP) Header Not Set (69)
Cross-Domain Misconfiguration (104)
Missing Anti-clickjacking Header (6)
Session ID in URL Rewrite (19)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (105)
Private IP Disclosure
Strict-Transport-Security Header Not Set
Timestamp Disclosure - Unix (174)
X-Content-Type-Options Header Missing (19)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (54)
Retrieved from Cache (14)
User Agent Fuzzer (126)
Vulnerable JS Library
URL: https://cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: /2.2.4/jquery.min.js
CWE ID: 1395
WASC ID:
Source: Passive (10003 - Vulnerable JS Library (Powered by Retire.js))
Input Vector:
Description:
The identified library appears to be vulnerable.
Other Info:
The identified library jquery, version 2.2.4 is vulnerable.
CVE-2020-11023
CVE-2020-11022
Solution:
Alerts 1 6 5 4 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0

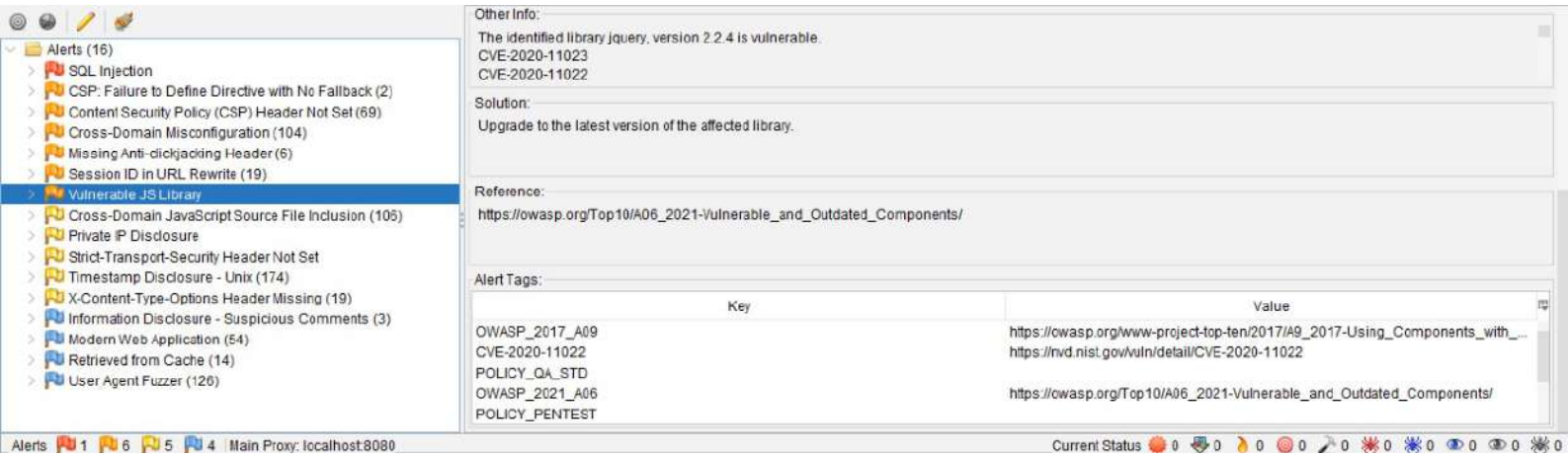

Alerts (16)
SQL Injection
CSP: Failure to Define Directive with No Fallback (2)
Content Security Policy (CSP) Header Not Set (69)
Cross-Domain Misconfiguration (104)
Missing Anti-clickjacking Header (6)
Session ID in URL Rewrite (19)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (106)
Private IP Disclosure
Strict-Transport-Security Header Not Set
Timestamp Disclosure - Unix (174)
X-Content-Type-Options Header Missing (19)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (54)
Retrieved from Cache (14)
User Agent Fuzzer (126)
Other Info:
Solution:
Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP
https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
https://www.w3.org/TR/CSP/
Alert Tags:
Key
Value
POLICY_QA_STD
POLICY_PENTEST
SYSTEMIC
https://www.zaproxy.org/docs/desktop/addons/common-library/alerttags/#systemic
CWE-693
https://cwe.mitre.org/data/definitions/693.html
OWASP_2017_A06
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.ht...
Alerts 1 6 5 4
Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0


localhost:3000/#/
Gmail
YouTube
Maps
Prayas 2.0 2023 - Ph...
Eduthoppee : Produ...
Adobe Acrobat
Cybersecurity
New folder
All Bookmarks
OWASP Juice Shop
Account
EN
All Products
Apple Juice (1000ml)
1.99¤
Apple Pomace
0.89¤
Banana Juice (1000ml)
1.99¤
This website uses fruit cookies to ensure you get the juiciest tracking experience.
But me wait!
Me want it!


History
Search
Alerts
Output
Active Scan
Spider
AJAX Spider
WebSockets
New Scan
Progress: 2: http://localhost:3000
76%
Current Scans: 1
URLs Found: 434
Nodes Added: 174
Export
URLs
Added Nodes
Messages
Processed
Method
URI
Flags
GET http://localhost:3000/assets/assets/assets/public/assets/public/assets/public/pol...
GET http://localhost:3000/assets/assets/assets/public/assets/public/assets/public/ven...
GET http://localhost:3000/assets/assets/assets/public/assets/public/assets/public/ma...
GET http://localhost:3000/assets/assets/public/assets/assets/public/assets/public/as...
GET http://localhost:3000/assets/assets/public/assets/assets/public/assets/public/as...
GET http://localhost:3000/assets/assets/public/assets/assets/public/assets/public/as...
GET http://localhost:3000/assets/assets/public/assets/assets/public/assets/public/as...
GET http://localhost:3000/assets/assets/public/assets/assets/public/assets/public/as...
GET http://localhost:3000/assets/assets/public/assets/assets/public/assets/public/as...
GET http://localhost:3000/assets/public/images/assets/public/assets/public/favicon_js...
GET http://localhost:3000/assets/public/images/assets/public/styles.css
GET http://localhost:3000/assets/public/images/assets/public/runtime.js
GET http://localhost:3000/assets/public/images/assets/public/polyfills.js
GET http://localhost:3000/assets/public/images/assets/public/vendor.js
GET http://localhost:3000/assets/public/images/assets/public/main.js
Alerts
Main Proxy: localhost:8080
Current Status


Alerts (16)
SQL Injection
CSP: Failure to Define Directive with No Fallback (2)
Content Security Policy (CSP) Header Not Set (69)
Cross-Domain Misconfiguration (104)
Missing Anti-clickjacking Header (6)
Session ID in URL Rewrite (19)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (105)
Private IP Disclosure
Strict-Transport-Security Header Not Set
Timestamp Disclosure - Unix (174)
X-Content-Type-Options Header Missing (19)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (54)
Retrieved from Cache (14)
User Agent Fuzzer (126)
Other Info:
The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP
Solution:
Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference:
https://vulncat.fortify.com/en/detail?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy
Alert Tags:
Key
Value
POLICY_QA_STD
POLICY_PENTEST
SYSTEMIC
https://www.zaproxy.org/docs/desktop/addons/common-library/alerttags/#systemic
OWASP_2017_A05
https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html
CWE-264
https://cwe.mitre.org/data/definitions/264.html
Alerts 1 6 5 4
Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0

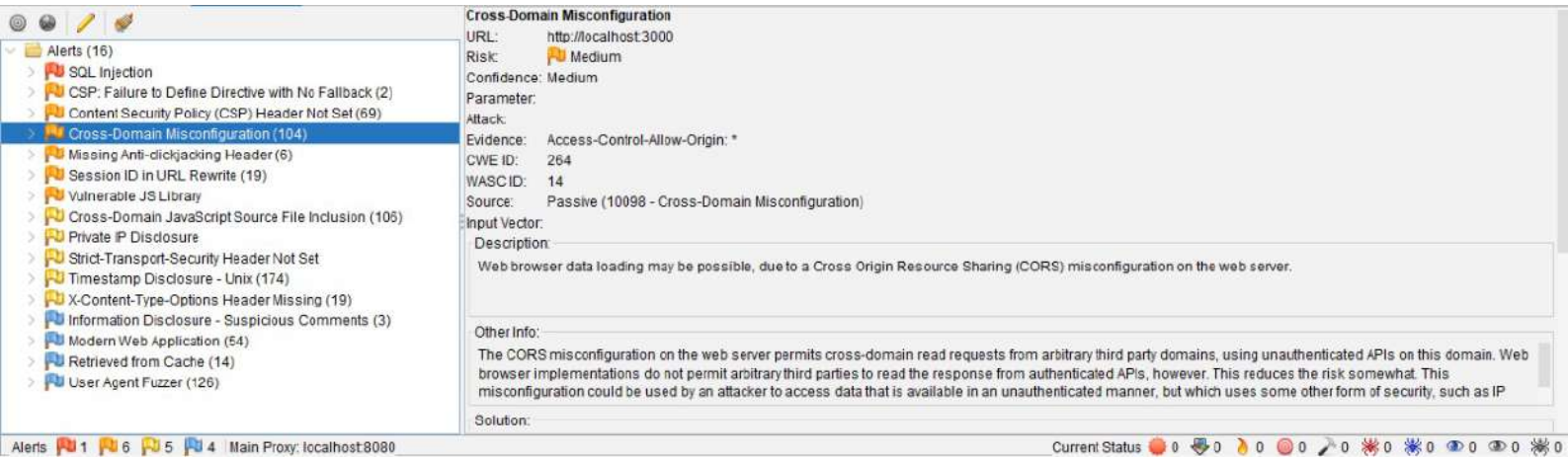

Alerts (16)
SQL Injection
CSP: Failure to Define Directive with No Fallback (2)
Content Security Policy (CSP) Header Not Set (69)
Cross-Domain Misconfiguration (104)
Missing Anti-clickjacking Header (6)
Session ID in URL Rewrite (19)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (106)
Private IP Disclosure
Strict-Transport-Security Header Not Set
Timestamp Disclosure - Unix (174)
X-Content-Type-Options Header Missing (19)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (54)
Retrieved from Cache (14)
User Agent Fuzzer (126)

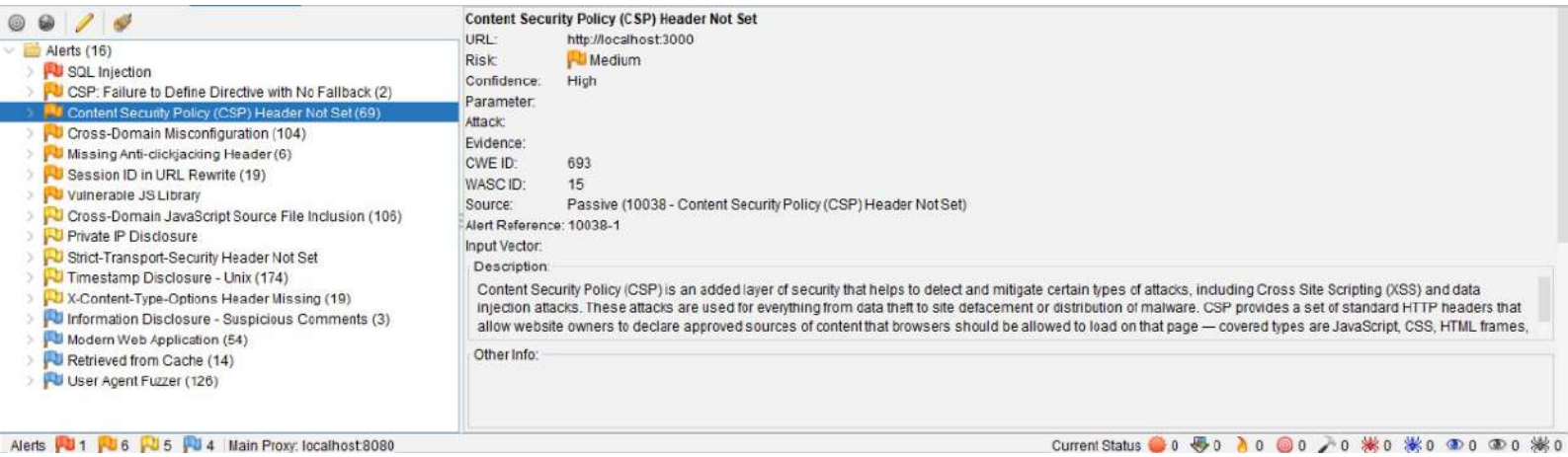

Alerts (16)
SQL Injection
CSP: Failure to Define Directive with No Fallback (2)
Content Security Policy (CSP) Header Not Set (69)
Cross-Domain Misconfiguration (104)
Missing Anti-clickjacking Header (6)
Session ID in URL Rewrite (19)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (105)
Private IP Disclosure
Strict-Transport-Security Header Not Set
Timestamp Disclosure - Unix (174)
X-Content-Type-Options Header Missing (19)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (54)
Retrieved from Cache (14)
User Agent Fuzzer (126)
Other Info:
The identified library jquery, version 2.2.4 is vulnerable.
CVE-2020-11023
CVE-2020-11022
Solution:
Upgrade to the latest version of the affected library.
Reference:
https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
Alert Tags:
Key
Value
OWASP_2017_A09
https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_...
CVE-2020-11022
https://nvd.nist.gov/vuln/detail/CVE-2020-11022
POLICY_QA_STD
OWASP_2021_A06
https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
POLICY_PENTEST
Alerts 1 6 5 4
Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0

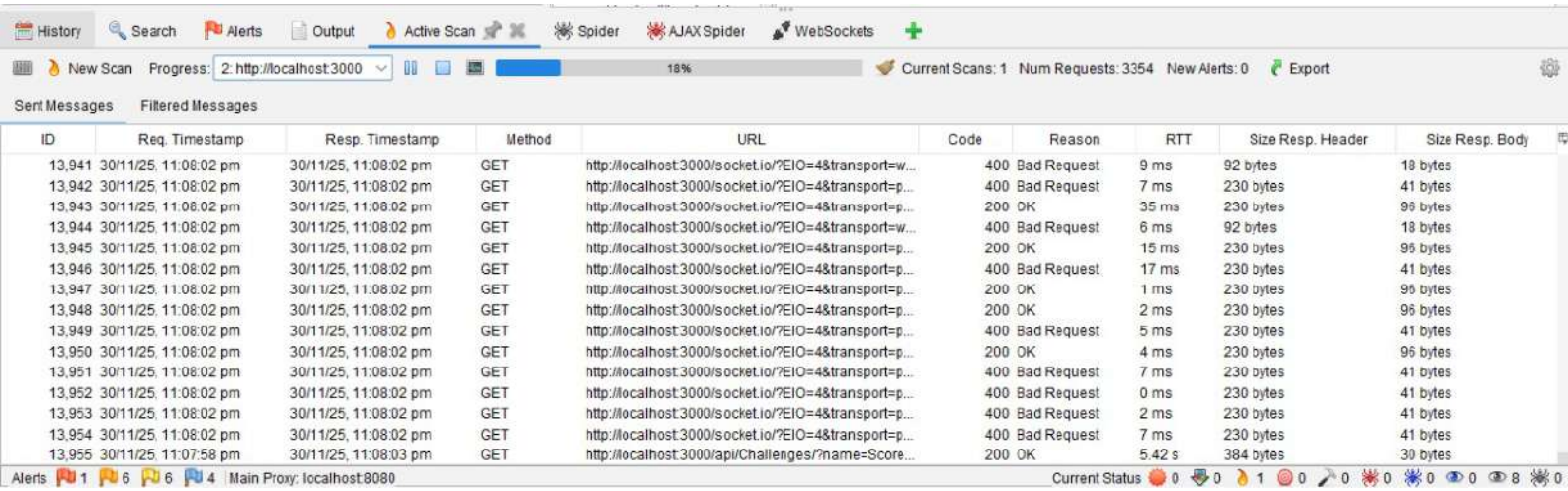

Alerts (16)
SQL Injection
CSP: Failure to Define Directive with No Fallback (2)
Content Security Policy (CSP) Header Not Set (69)
Cross-Domain Misconfiguration (104)
Missing Anti-clickjacking Header (6)
Session ID in URL Rewrite (19)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (106)
Private IP Disclosure
Strict-Transport-Security Header Not Set
Timestamp Disclosure - Unix (174)
X-Content-Type-Options Header Missing (19)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (54)
Retrieved from Cache (14)
User Agent Fuzzer (126)
Session ID in URL Rewrite
URL: http://localhost:3000/socket.io/?EIO=4&transport=websocket&sid=DguG04vq4DqRNy_6AAAC
Risk: Medium
Confidence: High
Parameter: sid
Attack:
Evidence: DguG04vq4DqRNy_6AAAC
CWE ID: 598
WASC ID: 13
Source: Passive (3 - Session ID in URL Rewrite)
Alert Reference: 3-1
Input Vector:
Description:
URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referer header. In addition, the session ID might be stored in browser history or server logs.
Other Info:
Alerts 1 6 5 4 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0


Alerts (16)
SQL Injection
CSP: Failure to Define Directive with No Fallback (2)
Content Security Policy (CSP) Header Not Set (69)
Cross-Domain Misconfiguration (104)
Missing Anti-clickjacking Header (6)
Session ID in URL Rewrite (19)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (105)
Private IP Disclosure
Strict-Transport-Security Header Not Set
Timestamp Disclosure - Unix (174)
X-Content-Type-Options Header Missing (19)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (54)
Retrieved from Cache (14)
User Agent Fuzzer (126)
Other Info:
Solution:
Do not trust client side input, even if there is client side validation in place.
In general, type check all data on the server side.
If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?'
Reference:
https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
Alert Tags:
Key
Value
POLICY_QA_FULL
POLICY_PENTEST
HIPAA
https://www.zaproxy.org/docs/desktop/addons/common-library/alerttags/#complia...
OWASP_2017_A01
https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html
POLICY_DEV_STD
Alerts 1 6 5 4
Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0


Alerts (16)
SQL Injection
CSP: Failure to Define Directive with No Fallback (2)
Content Security Policy (CSP) Header Not Set (69)
Cross-Domain Misconfiguration (104)
Missing Anti-clickjacking Header (6)
Session ID in URL Rewrite (19)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (105)
Private IP Disclosure
Strict-Transport-Security Header Not Set
Timestamp Disclosure - Unix (174)
X-Content-Type-Options Header Missing (19)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (54)
Retrieved from Cache (14)
User Agent Fuzzer (126)
Other Info:
Solution:
Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.
If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options
Alert Tags:
Key
Value
POLICY_QA_STD
POLICY_PENTEST
CWE-1021
https://cwe.mitre.org/data/definitions/1021.html
SYSTEMIC
https://www.zaproxy.org/docs/desktop/addons/common-library/alerttags/#systemic
WSTG-v42-CLNT-09
https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application...
Alerts 1 6 5 4
Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0


Alerts (16)
SQL Injection
CSP: Failure to Define Directive with No Fallback (2)
Content Security Policy (CSP) Header Not Set (69)
Cross-Domain Misconfiguration (104)
Missing Anti-clickjacking Header (6)
Session ID in URL Rewrite (19)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (105)
Private IP Disclosure
Strict-Transport-Security Header Not Set
Timestamp Disclosure - Unix (174)
X-Content-Type-Options Header Missing (19)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (54)
Retrieved from Cache (14)
User Agent Fuzzer (126)
Cross-Domain Misconfiguration
URL: http://localhost:3000
Risk: Medium
Confidence: Medium
Parameter:
Attack:
Evidence: Access-Control-Allow-Origin: *
CWE ID: 264
WASC ID: 14
Source: Passive (10098 - Cross-Domain Misconfiguration)
Input Vector:
Description:
Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
Other Info:
The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP
Solution:
Alerts 1 6 5 4 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0 0


Alerts (16)
SQL Injection
CSP: Failure to Define Directive with No Fallback (2)
Content Security Policy (CSP) Header Not Set (69)
Cross-Domain Misconfiguration (104)
Missing Anti-clickjacking Header (6)
Session ID in URL Rewrite (19)
Vulnerable JS Library
Cross-Domain JavaScript Source File Inclusion (105)
Private IP Disclosure
Strict-Transport-Security Header Not Set
Timestamp Disclosure - Unix (174)
X-Content-Type-Options Header Missing (19)
Information Disclosure - Suspicious Comments (3)
Modern Web Application (54)
Retrieved from Cache (14)
User Agent Fuzzer (126)
Content Security Policy (CSP) Header Not Set
URL: http://localhost:3000
Risk: Medium
Confidence: High
Parameter:
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Source: Passive (10038 - Content Security Policy (CSP) Header Not Set)
Alert Reference: 10038-1
Input Vector:
Description:
Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames,
Other Info:
Alerts 1 6 5 4 Main Proxy: localhost:8080
Current Status 0 0 0 0 0 0 0 0 0 0


History
Search
Alerts
Output
Active Scan
Spider
AJAX Spider
WebSockets
New Scan
Progress: 2: http://localhost:3000
18%
Current Scans: 1
Num Requests: 3354
New Alerts: 0
Export
Sent Messages
Filtered Messages
ID Req. Timestamp Resp. Timestamp Method URL Code Reason RTT Size Resp. Header Size Resp. Body
13,941 30/11/25, 11:08:02 pm 30/11/25, 11:08:02 pm GET http://localhost:3000/socket.io/?EIO=4&transport=w... 400 Bad Request 9 ms 92 bytes 18 bytes
13,942 30/11/25, 11:08:02 pm 30/11/25, 11:08:02 pm GET http://localhost:3000/socket.io/?EIO=4&transport=p... 400 Bad Request 7 ms 230 bytes 41 bytes
13,943 30/11/25, 11:08:02 pm 30/11/25, 11:08:02 pm GET http://localhost:3000/socket.io/?EIO=4&transport=p... 200 OK 35 ms 230 bytes 96 bytes
13,944 30/11/25, 11:08:02 pm 30/11/25, 11:08:02 pm GET http://localhost:3000/socket.io/?EIO=4&transport=w... 400 Bad Request 6 ms 92 bytes 18 bytes
13,945 30/11/25, 11:08:02 pm 30/11/25, 11:08:02 pm GET http://localhost:3000/socket.io/?EIO=4&transport=p... 200 OK 15 ms 230 bytes 96 bytes
13,946 30/11/25, 11:08:02 pm 30/11/25, 11:08:02 pm GET http://localhost:3000/socket.io/?EIO=4&transport=p... 400 Bad Request 17 ms 230 bytes 41 bytes
13,947 30/11/25, 11:08:02 pm 30/11/25, 11:08:02 pm GET http://localhost:3000/socket.io/?EIO=4&transport=p... 200 OK 1 ms 230 bytes 96 bytes
13,948 30/11/25, 11:08:02 pm 30/11/25, 11:08:02 pm GET http://localhost:3000/socket.io/?EIO=4&transport=p... 200 OK 2 ms 230 bytes 96 bytes
13,949 30/11/25, 11:08:02 pm 30/11/25, 11:08:02 pm GET http://localhost:3000/socket.io/?EIO=4&transport=p... 400 Bad Request 5 ms 230 bytes 41 bytes
13,950 30/11/25, 11:08:02 pm 30/11/25, 11:08:02 pm GET http://localhost:3000/socket.io/?EIO=4&transport=p... 200 OK 4 ms 230 bytes 96 bytes
13,951 30/11/25, 11:08:02 pm 30/11/25, 11:08:02 pm GET http://localhost:3000/socket.io/?EIO=4&transport=p... 400 Bad Request 7 ms 230 bytes 41 bytes
13,952 30/11/25, 11:08:02 pm 30/11/25, 11:08:02 pm GET http://localhost:3000/socket.io/?EIO=4&transport=p... 400 Bad Request 0 ms 230 bytes 41 bytes
13,953 30/11/25, 11:08:02 pm 30/11/25, 11:08:02 pm GET http://localhost:3000/socket.io/?EIO=4&transport=p... 400 Bad Request 2 ms 230 bytes 41 bytes
13,954 30/11/25, 11:08:02 pm 30/11/25, 11:08:02 pm GET http://localhost:3000/socket.io/?EIO=4&transport=p... 400 Bad Request 7 ms 230 bytes 41 bytes
13,955 30/11/25, 11:07:58 pm 30/11/25, 11:08:03 pm GET http://localhost:3000/api/Challenges/?name=Score... 200 OK 5.42 s 384 bytes 30 bytes
Alerts 1 6 6 4 Main Proxy: localhost:8080
Current Status 0 0 1 0 0 0 0 0 0 8 0