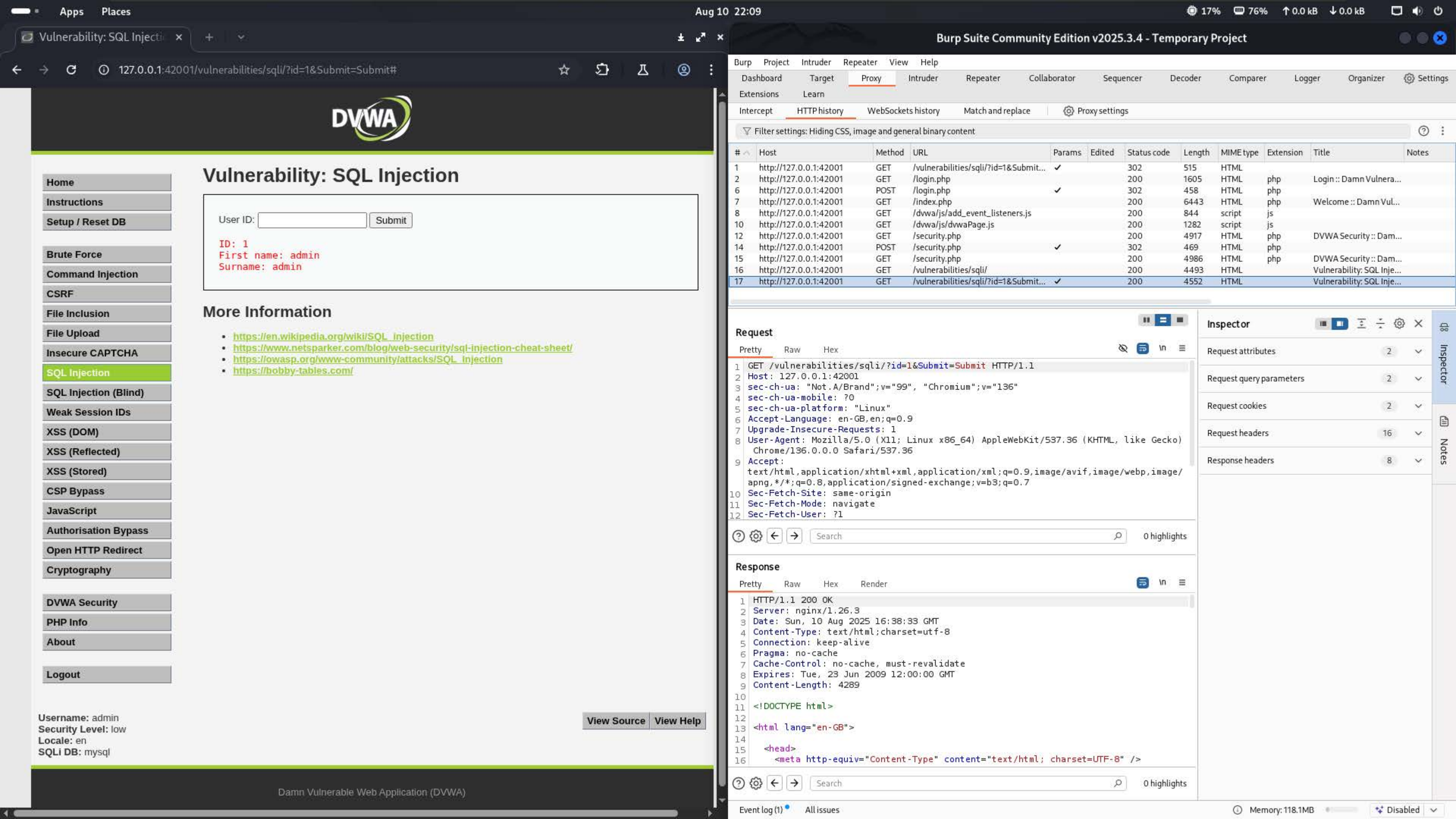
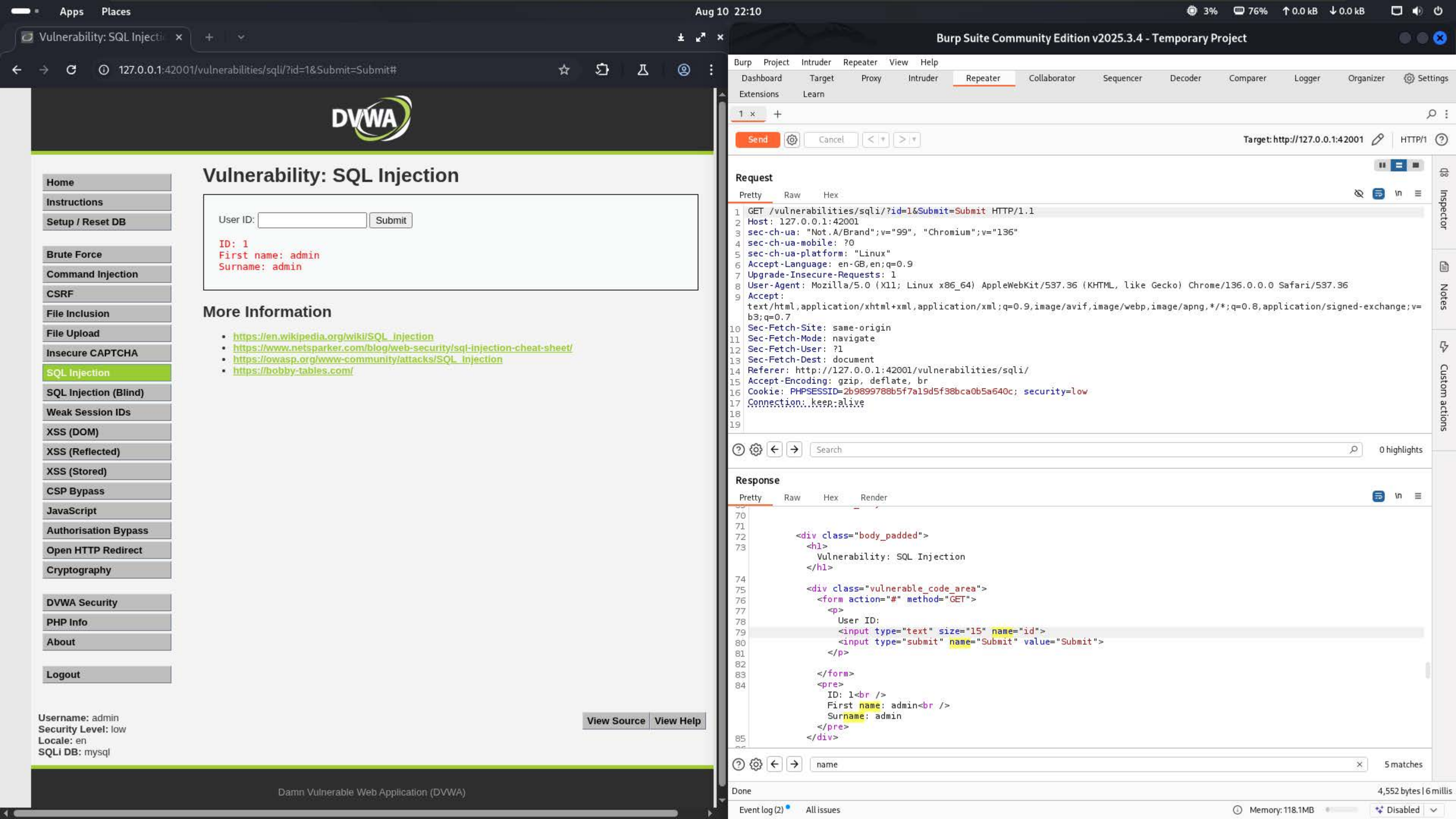

Apps Places
Aug 10 22:09
17% 76% 0.0 kB 0.0 kB
Vulnerability: SQL Injecti
127.0.0.1:42001/vulnerabilities/sqli/?id=1&Submit=Submit#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID:
Submit
ID: 1
First name: admin
Surname: admin
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source
View Help
Damn Vulnerable Web Application (DVWA)
Burp Suite Community Edition v2025.3.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Filter settings: Hiding CSS, image and general binary content
Host Method URL Params Edited Status code Length MIME type Extension Title Notes
1 http://127.0.0.1:42001 GET /vulnerabilities/sqli/?id=1&Submit... ✓ 302 515 HTML
2 http://127.0.0.1:42001 GET /login.php 200 1605 HTML php Login :: Damn Vulnera...
6 http://127.0.0.1:42001 POST /login.php ✓ 302 458 HTML php
7 http://127.0.0.1:42001 GET /index.php 200 6443 HTML php Welcome :: Damn Vul...
8 http://127.0.0.1:42001 GET /dvwa/js/add_event_listeners.js 200 844 script js
10 http://127.0.0.1:42001 GET /dvwa/js/dvwaPage.js 200 1282 script js
12 http://127.0.0.1:42001 GET /security.php 200 4917 HTML php DVWA Security :: Dam...
14 http://127.0.0.1:42001 POST /security.php ✓ 302 469 HTML php
15 http://127.0.0.1:42001 GET /security.php 200 4986 HTML php DVWA Security :: Dam...
16 http://127.0.0.1:42001 GET /vulnerabilities/sqli/ 200 4493 HTML Vulnerability: SQL Inje...
17 http://127.0.0.1:42001 GET /vulnerabilities/sqli/?id=1&Submit... ✓ 200 4552 HTML Vulnerability: SQL Inje...
Request
Pretty Raw Hex
1 GET /vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
2 Host: 127.0.0.1:42001
3 sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Accept-Language: en-GB,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 Safari/537.36
9 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=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
Search 0 highlights
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Server: nginx/1.26.3
3 Date: Sun, 10 Aug 2025 16:38:33 GMT
4 Content-Type: text/html;charset=utf-8
5 Connection: keep-alive
6 Pragma: no-cache
7 Cache-Control: no-cache, must-revalidate
8 Expires: Tue, 23 Jun 2009 12:00:00 GMT
9 Content-Length: 4289
10
11 <!DOCTYPE html>
12
13 <html lang="en-GB">
14
15 <head>
16 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
Search 0 highlights
Inspector
Request attributes 2
Request query parameters 2
Request cookies 2
Request headers 16
Response headers 8
Inspector
Notes
Event log (1) All issues
Memory: 118.1MB
Disabled


Apps Places
Aug 10 22:10
3% 76% 0.0 kB 0.0 kB
Vulnerability: SQL Injecti
127.0.0.1:42001/vulnerabilities/sqli/?id=1&Submit=Submit#
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Authorisation Bypass
Open HTTP Redirect
Cryptography
DVWA Security
PHP Info
About
Logout
Vulnerability: SQL Injection
User ID: Submit
ID: 1
First name: admin
Surname: admin
More Information
https://en.wikipedia.org/wiki/SQL_injection
https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
https://owasp.org/www-community/attacks/SQL_Injection
https://bobby-tables.com/
Username: admin
Security Level: low
Locale: en
SQLi DB: mysql
View Source View Help
Damn Vulnerable Web Application (DVWA)
Burp Suite Community Edition v2025.3.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Send Cancel
Target: http://127.0.0.1:42001 HTTP/1
Request
Pretty Raw Hex
GET /vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
Host: 127.0.0.1:42001
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1:42001/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=2b9899788b5f7a19d5f38bca0b5a640c; security=low
Connection: keep-alive
Search 0 highlights
Response
Pretty Raw Hex Render

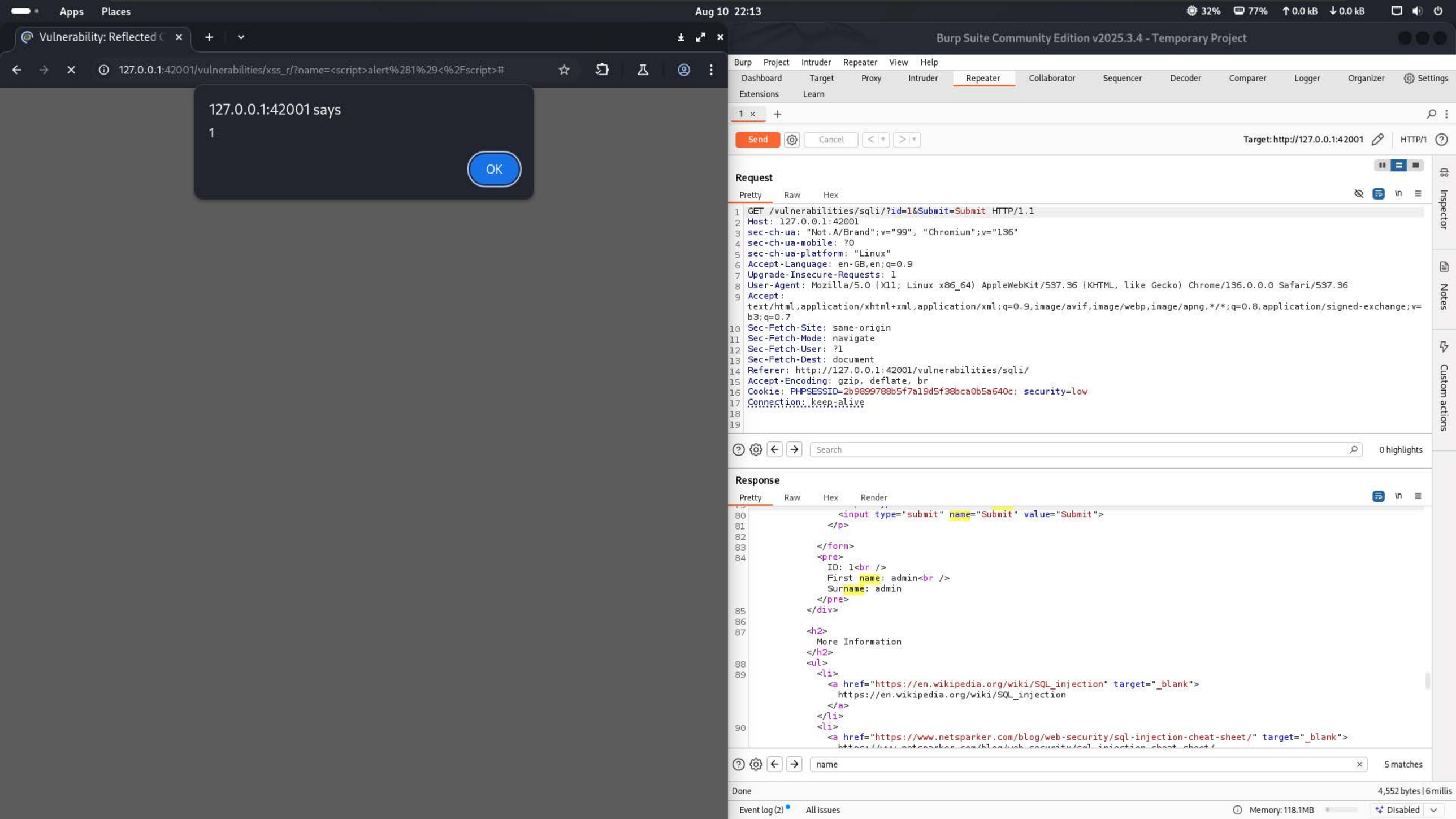
<h1>
Vulnerability: SQL Injection
</h1>

<form action="#" method="GET">

User ID:
<input type="text" size="15" name="id">
<input type="submit" name="Submit" value="Submit">

</form>
<pre>
ID: 1
First name: admin
Surname: admin
</pre>

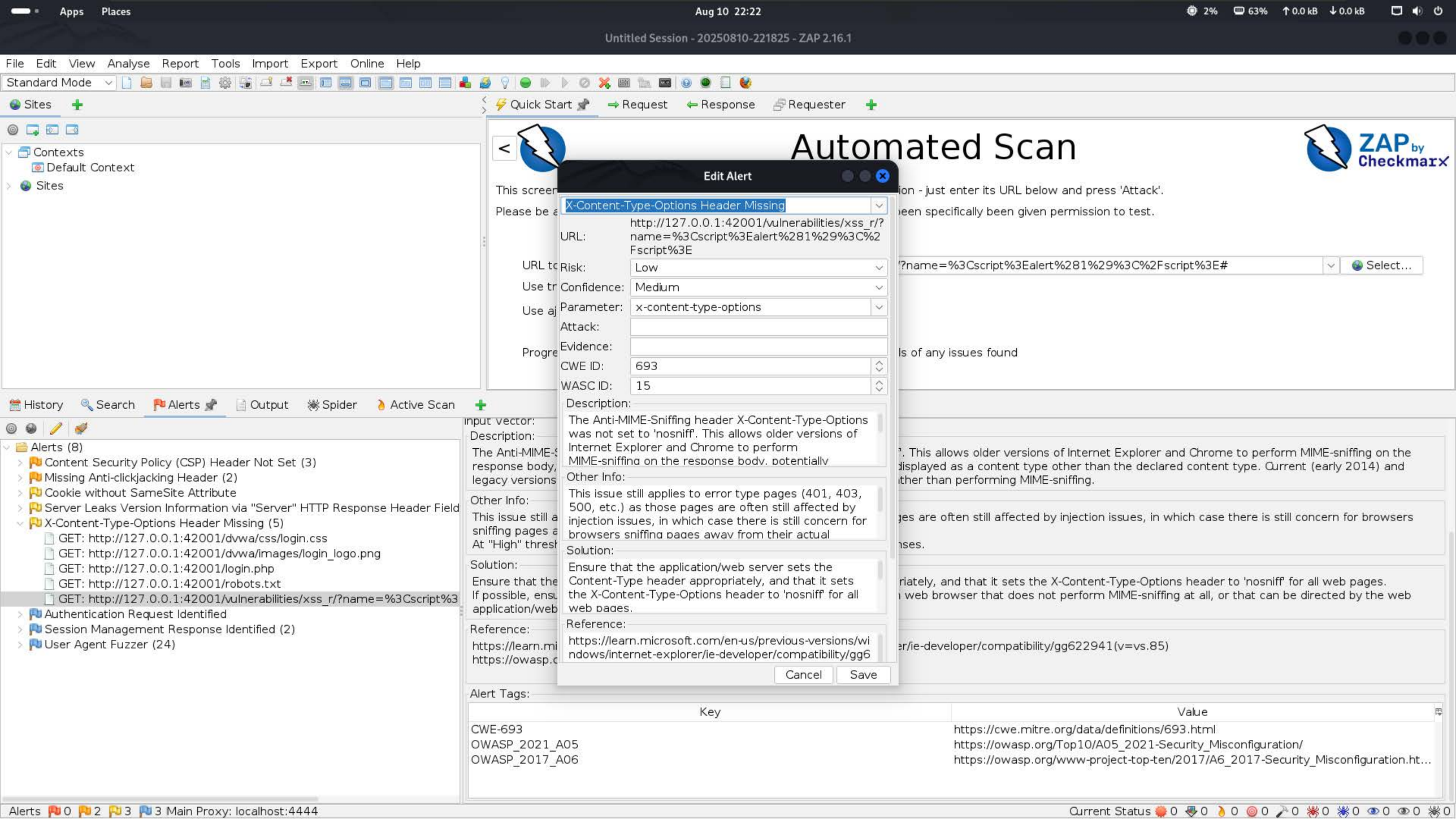
name 5 matches
Done 4,552 bytes | 6 millis
Event log (2) All issues
Memory: 118.1MB Disabled
Inspector
Notes
Custom actions


Apps
Places
Aug 10 22:13
32%
77%
0.0 kB
0.0 kB
Vulnerability: Reflected
127.0.0.1:42001/vulnerabilities/xss_r/?name=<script>alert%281%29<%2Fscript>#
127.0.0.1:42001 says
1
OK
Burp Suite Community Edition v2025.3.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Send Cancel
Target: http://127.0.0.1:42001
HTTP/1
Request
Pretty Raw Hex
GET /vulnerabilities/sqli/?id=1&Submit=Submit HTTP/1.1
Host: 127.0.0.1:42001
sec-ch-ua: "Not.A/Brand";v="99", "Chromium";v="136"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/136.0.0.0 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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1:42001/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, br
Cookie: PHPSESSID=2b9899788b5f7a19d5f38bca0b5a640c; security=low
Connection: keep-alive
Search
0 highlights
Response
Pretty Raw Hex Render
<input type="submit" name="Submit" value="Submit">
</p>
</form>
<pre>
ID: 1
First name: admin
Surname: admin
</pre>

<h2>
More Information
</h2>

https://en.wikipedia.org/wiki/SQL_injection

<a href="https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/" target="_blank">
name
5 matches
Done
4,552 bytes | 6 millis
Event log (2)
All issues
Memory: 118.1MB
Disabled
Inspector
Notes
Custom actions


Apps Places
Aug 10 22:22
2% 63% 0.0 kB 0.0 kB
Untitled Session - 20250810-221825 - ZAP 2.16.1
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
Automated Scan
ZAP by Checkmarx
Edit Alert
X-Content-Type-Options Header Missing
URL: http://127.0.0.1:42001/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%281%29%3C%2Fscript%3E
Risk: Low
Confidence: Medium
Parameter: x-content-type-options
Attack:
Evidence:
CWE ID: 693
WASC ID: 15
Description:
The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially
Other Info:
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual
Solution:
Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.
Reference:
https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg6
Cancel
Save
Select...
History
Search
Alerts
Output
Spider
Active Scan
Alerts (8)
Content Security Policy (CSP) Header Not Set (3)
Missing Anti-clickjacking Header (2)
Cookie without SameSite Attribute
Server Leaks Version Information via "Server" HTTP Response Header Field
X-Content-Type-Options Header Missing (5)
GET: http://127.0.0.1:42001/dvwa/css/login.css
GET: http://127.0.0.1:42001/dvwa/images/login_logo.png
GET: http://127.0.0.1:42001/login.php
GET: http://127.0.0.1:42001/robots.txt
GET: http://127.0.0.1:42001/vulnerabilities/xss_r/?name=%3Cscript%3
Authentication Request Identified
Session Management Response Identified (2)
User Agent Fuzzer (24)
Alert Tags:
Key
Value
CWE-693
https://cwe.mitre.org/data/definitions/693.html
OWASP_2021_A05
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
OWASP_2017_A06
https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.ht...
Alerts 0 2 3 3 Main Proxy: localhost:4444
Current Status 0 0 0 0 0 0 0 0 0 0