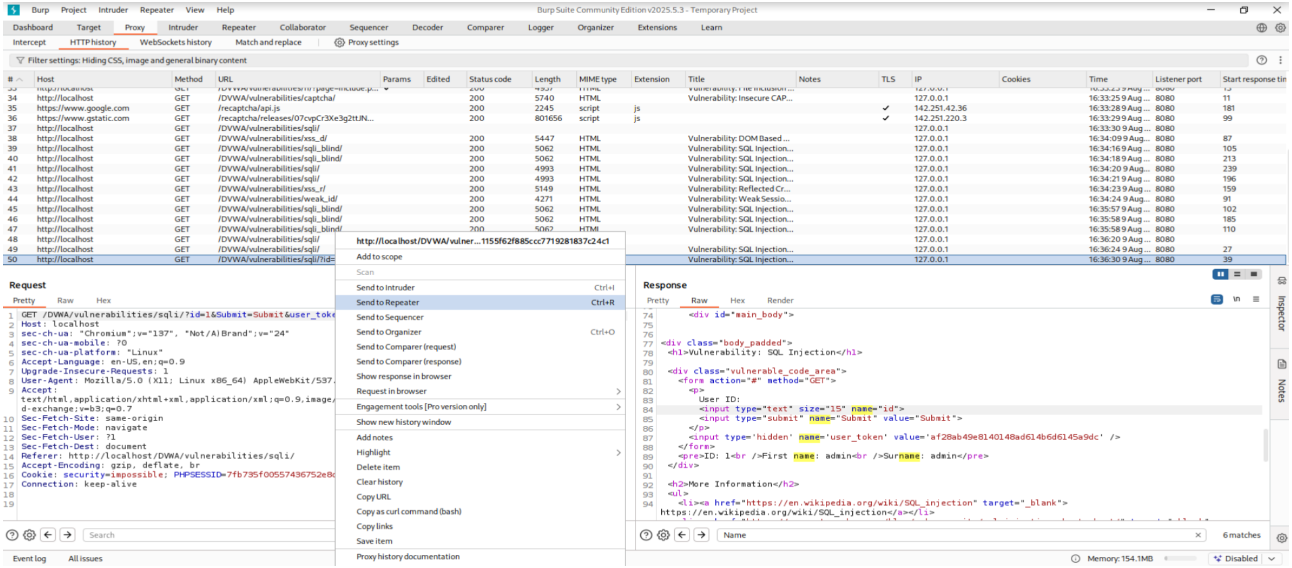
Future Interns - Task 1 Screenshots & Descriptions

Screenshot 1: Burp Suite SQL Injection Capture

Captured HTTP request and response in Burp Suite showing SQL Injection attempt via 'id' parameter.


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.3 - 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, image and general binary content
http://localhost/DVWA/vulner...1155f62f885ccc7719281837c24c1
Add to scope
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Organizer Ctrl+O
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
Engagement tools [Pro version only]
Show new history window
Add notes
Highlight
Delete item
Clear history
Copy URL
Copy as curl command (bash)
Copy links
Save item
Proxy history documentation
Request
Pretty Raw Hex
Search
Response
Pretty Raw Hex Render
Name
6 matches
Inspector
Notes
Event log All issues
Memory: 154.1MB
Disabled

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response tim
34	http://localhost	GET	/DVWA/vulnerabilities/captcha/			200	5740	HTML		Vulnerability: Insecure CAP...			127.0.0.1		16:33:25 9 Aug ...	8080	11
35	https://www.google.com	GET	/recaptcha/api.js			200	2245	script	js			✓	142.251.42.36		16:33:28 9 Aug ...	8080	181
36	https://www.gstatic.com	GET	/recaptcha/releases/07cvpCr3Xe3g2ttJN...			200	801656	script	js			✓	142.251.220.3		16:33:29 9 Aug ...	8080	99
37	http://localhost	GET	/DVWA/vulnerabilities/sqli/										127.0.0.1		16:33:30 9 Aug ...	8080	
38	http://localhost	GET	/DVWA/vulnerabilities/xss_d/			200	5447	HTML		Vulnerability: DOM Based ...			127.0.0.1		16:34:09 9 Aug...	8080	87
39	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:34:16 9 Aug ...	8080	105
40	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:34:18 9 Aug ...	8080	213
41	http://localhost	GET	/DVWA/vulnerabilities/sqli/			200	4993	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:34:20 9 Aug...	8080	239
42	http://localhost	GET	/DVWA/vulnerabilities/sqli/			200	4993	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:34:21 9 Aug ...	8080	196
43	http://localhost	GET	/DVWA/vulnerabilities/xss_r/			200	5149	HTML		Vulnerability: Reflected Cr...			127.0.0.1		16:34:23 9 Aug ...	8080	159
44	http://localhost	GET	/DVWA/vulnerabilities/weak_id/			200	4271	HTML		Vulnerability: Weak Sessio...			127.0.0.1		16:34:24 9 Aug...	8080	91
45	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:35:57 9 Aug ...	8080	102
46	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:35:58 9 Aug ...	8080	185
47	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:35:58 9 Aug ...	8080	110
48	http://localhost	GET	/DVWA/vulnerabilities/sqli/										127.0.0.1		16:36:20 9 Aug ...	8080	
49	http://localhost	GET	/DVWA/vulnerabilities/sqli/							Vulnerability: SQL Injection...			127.0.0.1		16:36:24 9 Aug ...	8080	27
50	http://localhost	GET	/DVWA/vulnerabilities/sqli/?id=							Vulnerability: SQL Injection...			127.0.0.1		16:36:30 9 Aug ...	8080	39

Request

```
GET /DVWA/vulnerabilities/sqli/?id=1&Submit=Submit&user_toke
Host: localhost
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
d-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://localhost/DVWA/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=7fb735f00557436752e8c
Connection: keep-alive
```

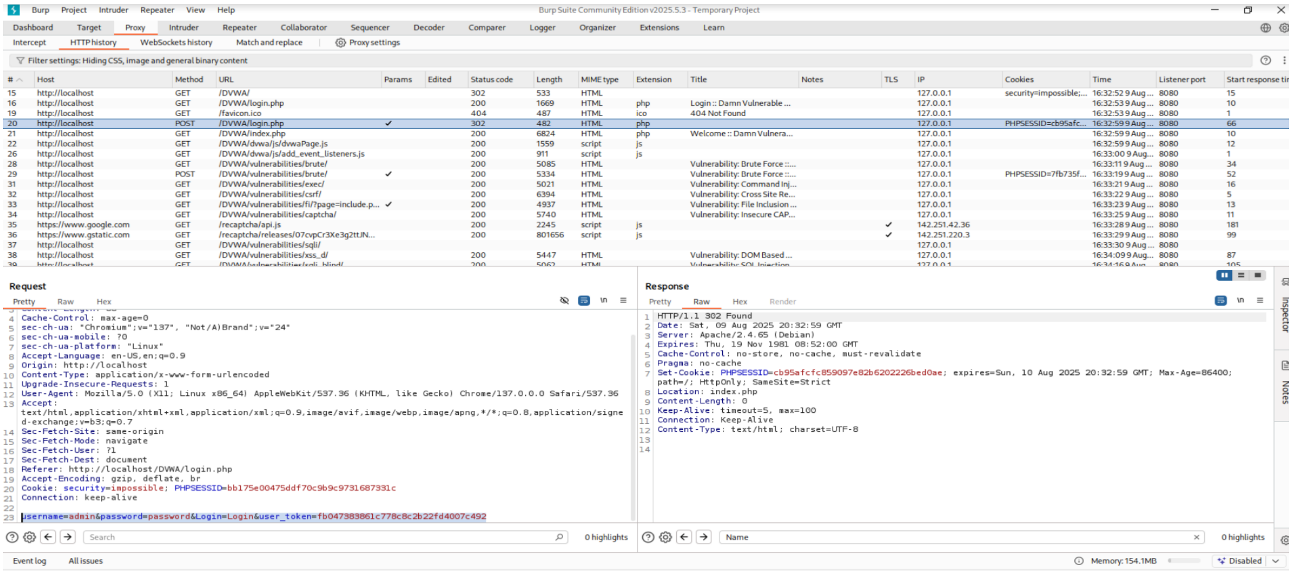
Response

```
      <div id="main_body">


<div class="body_padded">
  <h1>Vulnerability: SQL Injection</h1>

  <div class="vulnerable_code_area">
    <form action="#" method="GET">
      <p>
        User ID:
        <input type="text" size="15" name="id">
        <input type="submit" name="Submit" value="Submit">
      </p>
      <input type='hidden' name='user_token' value='af28ab49e8140148ad614b6d6145a9dc' />
    </form>
    <pre>ID: 1<br />First name: admin<br />Surname: admin</pre>
  </div>

  <h2>More Information</h2>
  <ul>
    <li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">
https://en.wikipedia.org/wiki/SQL_injection</a></li>
```

Future Interns - Task 1 Screenshots & Descriptions

Screenshot 2: Burp Suite Login Capture

Burp Suite intercept showing successful login request and server response redirection.



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response tir
15	http://localhost	GET	/DVWA/			302	533	HTML					127.0.0.1	security=impossible;...	16:32:52 9 Aug ...	8080	15
16	http://localhost	GET	/DVWA/login.php			200	1669	HTML	php	Login :: Damn Vulnerable ...			127.0.0.1		16:32:53 9 Aug ...	8080	10
19	http://localhost	GET	/favicon.ico			404	487	HTML	ico	404 Not Found			127.0.0.1		16:32:53 9 Aug ...	8080	1
20	http://localhost	POST	/DVWA/login.php	✓		302	482	HTML	php				127.0.0.1	PHPSESSID=cb95afc...	16:32:59 9 Aug ...	8080	66
21	http://localhost	GET	/DVWA/index.php			200	6824	HTML	php	Welcome :: Damn Vulnera...			127.0.0.1		16:32:59 9 Aug ...	8080	10
22	http://localhost	GET	/DVWA/dvwa/js/dvwaPage.js			200	1559	script	js				127.0.0.1		16:32:59 9 Aug ...	8080	12
26	http://localhost	GET	/DVWA/dvwa/js/add_event_listeners.js			200	911	script	js				127.0.0.1		16:33:00 9 Aug...	8080	1
28	http://localhost	GET	/DVWA/vulnerabilities/brute/			200	5085	HTML		Vulnerability: Brute Force ::...			127.0.0.1		16:33:11 9 Aug ...	8080	34
29	http://localhost	POST	/DVWA/vulnerabilities/brute/	✓		200	5334	HTML		Vulnerability: Brute Force ::...			127.0.0.1	PHPSESSID=7fb735f...	16:33:19 9 Aug ...	8080	52
31	http://localhost	GET	/DVWA/vulnerabilities/exec/			200	5021	HTML		Vulnerability: Command Inj...			127.0.0.1		16:33:21 9 Aug ...	8080	16
32	http://localhost	GET	/DVWA/vulnerabilities/csrf/			200	6394	HTML		Vulnerability: Cross Site Re...			127.0.0.1		16:33:22 9 Aug ...	8080	5
33	http://localhost	GET	/DVWA/vulnerabilities/fi/?page=include.p...	✓		200	4937	HTML		Vulnerability: File Inclusion ...			127.0.0.1		16:33:23 9 Aug ...	8080	13
34	http://localhost	GET	/DVWA/vulnerabilities/captcha/			200	5740	HTML		Vulnerability: Insecure CAP...			127.0.0.1		16:33:25 9 Aug ...	8080	11
35	https://www.google.com	GET	/recaptcha/api.js			200	2245	script	js			✓	142.251.42.36		16:33:28 9 Aug ...	8080	181
36	https://www.gstatic.com	GET	/recaptcha/releases/07cvpCr3Xe3g2ttJN...			200	801656	script	js			✓	142.251.220.3		16:33:29 9 Aug ...	8080	99
37	http://localhost	GET	/DVWA/vulnerabilities/sqli/										127.0.0.1		16:33:30 9 Aug ...	8080	
38	http://localhost	GET	/DVWA/vulnerabilities/xss_d/			200	5447	HTML		Vulnerability: DOM Based ...			127.0.0.1		16:34:09 9 Aug...	8080	87
39	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection ...			127.0.0.1		16:34:16 9 Aug ...	8080	105

Request

```
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 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://localhost/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=bb175e00475ddf70c9b9c9731687331c
Connection: keep-alive

username=admin&password=password&Login=Login&user_token=fb047383861c778c8c2b22fd4007c492
```

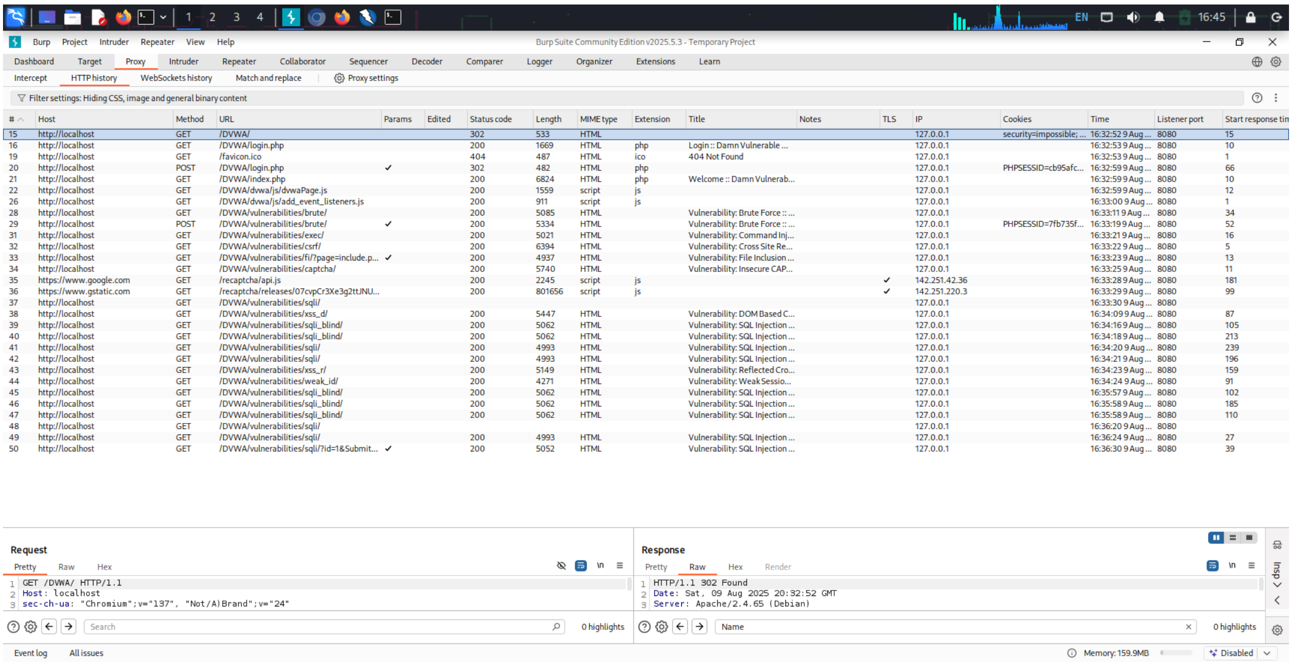
Response

```
HTTP/1.1 302 Found
Date: Sat, 09 Aug 2025 20:32:59 GMT
Server: Apache/2.4.65 (Debian)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=cb95afcfc859097e82b6202226bed0ae; expires=Sun, 10 Aug 2025 20:32:59 GMT; Max-Age=86400;
path=/; HttpOnly; SameSite=Strict
Location: index.php
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Future Interns - Task 1 Screenshots & Descriptions

Screenshot 6: Burp Suite Target Overview

Complete Burp Suite proxy log of DVWA vulnerabilities, including SQL Injection and XSS endpoints.



1 2 3 4
EN 16:45
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.3 - 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
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Search
0 highlights
Name
0 highlights
Inspector
Event log All issues
Memory: 159.9MB
Disabled

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response tim
15	http://localhost	GET	/DVWA/			302	533	HTML					127.0.0.1	security=impossible; ...	16:32:52 9 Aug ...	8080	15
16	http://localhost	GET	/DVWA/login.php			200	1669	HTML	php	Login :: Damn Vulnerable ...			127.0.0.1		16:32:53 9 Aug ...	8080	10
19	http://localhost	GET	/favicon.ico			404	487	HTML	ico	404 Not Found			127.0.0.1		16:32:53 9 Aug ...	8080	1
20	http://localhost	POST	/DVWA/login.php	✓		302	482	HTML	php				127.0.0.1	PHPSESSID=cb95afc...	16:32:59 9 Aug ...	8080	66
21	http://localhost	GET	/DVWA/index.php			200	6824	HTML	php	Welcome :: Damn Vulnerab...			127.0.0.1		16:32:59 9 Aug ...	8080	10
22	http://localhost	GET	/DVWA/dvwa/js/dvwaPage.js			200	1559	script	js				127.0.0.1		16:32:59 9 Aug ...	8080	12
26	http://localhost	GET	/DVWA/dvwa/js/add_event_listeners.js			200	911	script	js				127.0.0.1		16:33:00 9 Aug ...	8080	1
28	http://localhost	GET	/DVWA/vulnerabilities/brute/			200	5085	HTML		Vulnerability: Brute Force :: ...			127.0.0.1		16:33:11 9 Aug ...	8080	34
29	http://localhost	POST	/DVWA/vulnerabilities/brute/	✓		200	5334	HTML		Vulnerability: Brute Force :: ...			127.0.0.1	PHPSESSID=7fb735f...	16:33:19 9 Aug ...	8080	52
31	http://localhost	GET	/DVWA/vulnerabilities/exec/			200	5021	HTML		Vulnerability: Command Inj...			127.0.0.1		16:33:21 9 Aug ...	8080	16
32	http://localhost	GET	/DVWA/vulnerabilities/csrf/			200	6394	HTML		Vulnerability: Cross Site Re...			127.0.0.1		16:33:22 9 Aug ...	8080	5
33	http://localhost	GET	/DVWA/vulnerabilities/fi/?page=include.p...	✓		200	4937	HTML		Vulnerability: File Inclusion ...			127.0.0.1		16:33:23 9 Aug ...	8080	13
34	http://localhost	GET	/DVWA/vulnerabilities/captcha/			200	5740	HTML		Vulnerability: Insecure CAP...			127.0.0.1		16:33:25 9 Aug ...	8080	11
35	https://www.google.com	GET	/recaptcha/api.js			200	2245	script	js			✓	142.251.42.36		16:33:28 9 Aug ...	8080	181
36	https://www.gstatic.com	GET	/recaptcha/releases/07cvpCr3Xe3g2ttJNU...			200	801656	script	js			✓	142.251.220.3		16:33:29 9 Aug ...	8080	99
37	http://localhost	GET	/DVWA/vulnerabilities/sqli/										127.0.0.1		16:33:30 9 Aug ...	8080	
38	http://localhost	GET	/DVWA/vulnerabilities/xss_d/			200	5447	HTML		Vulnerability: DOM Based C...			127.0.0.1		16:34:09 9 Aug ...	8080	87
39	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection ...			127.0.0.1		16:34:16 9 Aug ...	8080	105
40	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection ...			127.0.0.1		16:34:18 9 Aug ...	8080	213
41	http://localhost	GET	/DVWA/vulnerabilities/sqli/			200	4993	HTML		Vulnerability: SQL Injection ...			127.0.0.1		16:34:20 9 Aug ...	8080	239
42	http://localhost	GET	/DVWA/vulnerabilities/sqli/			200	4993	HTML		Vulnerability: SQL Injection ...			127.0.0.1		16:34:21 9 Aug ...	8080	196
43	http://localhost	GET	/DVWA/vulnerabilities/xss_r/			200	5149	HTML		Vulnerability: Reflected Cro...			127.0.0.1		16:34:23 9 Aug ...	8080	159
44	http://localhost	GET	/DVWA/vulnerabilities/weak_id/			200	4271	HTML		Vulnerability: Weak Sessio...			127.0.0.1		16:34:24 9 Aug ...	8080	91
45	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection ...			127.0.0.1		16:35:57 9 Aug ...	8080	102
46	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection ...			127.0.0.1		16:35:58 9 Aug ...	8080	185
47	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection ...			127.0.0.1		16:35:58 9 Aug ...	8080	110
48	http://localhost	GET	/DVWA/vulnerabilities/sqli/										127.0.0.1		16:36:20 9 Aug ...	8080	
49	http://localhost	GET	/DVWA/vulnerabilities/sqli/			200	4993	HTML		Vulnerability: SQL Injection ...			127.0.0.1		16:36:24 9 Aug ...	8080	27
50	http://localhost	GET	/DVWA/vulnerabilities/sqli/?id=1&Submit...	✓		200	5052	HTML		Vulnerability: SQL Injection ...			127.0.0.1		16:36:30 9 Aug ...	8080	39

Request

```
GET /DVWA/ HTTP/1.1
Host: localhost
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
```

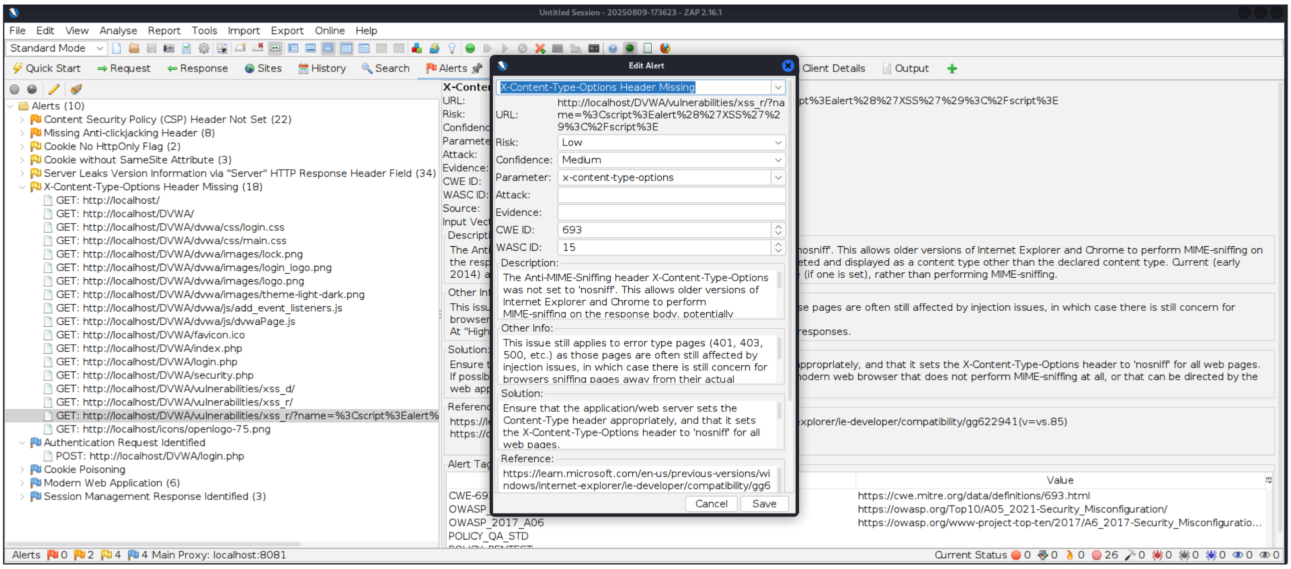
Response

```
HTTP/1.1 302 Found
Date: Sat, 09 Aug 2025 20:32:52 GMT
Server: Apache/2.4.65 (Debian)
```

Future Interns - Task 1 Screenshots & Descriptions

Screenshot 3: OWASP ZAP Scan Alert

OWASP ZAP scan reporting multiple security header issues and vulnerability alerts.



- Alerts (10)
  - Content Security Policy (CSP) Header Not Set (22)
  - Missing Anti-clickjacking Header (8)
  - Cookie No HttpOnly Flag (2)
  - Cookie without SameSite Attribute (3)
  - Server Leaks Version Information via "Server" HTTP Response Header Field (34)
  - X-Content-Type-Options Header Missing (18)
    - GET: http://localhost/
    - GET: http://localhost/DVWA/
    - GET: http://localhost/DVWA/dvwa/css/login.css
    - GET: http://localhost/DVWA/dvwa/css/main.css
    - GET: http://localhost/DVWA/dvwa/images/lock.png
    - GET: http://localhost/DVWA/dvwa/images/login_logo.png
    - GET: http://localhost/DVWA/dvwa/images/logo.png
    - GET: http://localhost/DVWA/dvwa/images/theme-light-dark.png
    - GET: http://localhost/DVWA/dvwa/js/add_event_listeners.js
    - GET: http://localhost/DVWA/dvwa/js/dvwaPage.js
    - GET: http://localhost/DVWA/favicon.ico
    - GET: http://localhost/DVWA/index.php
    - GET: http://localhost/DVWA/login.php
    - GET: http://localhost/DVWA/security.php
    - GET: http://localhost/DVWA/vulnerabilities/xss_d/
    - GET: http://localhost/DVWA/vulnerabilities/xss_r/
    - GET: http://localhost/DVWA/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%
    - GET: http://localhost/icons/openlogo-75.png
  - Authentication Request Identified
    - POST: http://localhost/DVWA/login.php
  - Cookie Poisoning
  - Modern Web Application (6)
  - Session Management Response Identified (3)

X-Conte
URL: ... pt%3Ealert%28%27XSS%27%29%3C%2Fscript%3E
Risk:
Confidenc
Paramete
Attack:
Evidence:
CWE ID:
WASC ID:
Source:
Input Vect

Descripti
The Anti ... nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on
the resp ... eted and displayed as a content type other than the declared content type. Current (early
2014) a ... (if one is set), rather than performing MIME-sniffing.

Other Inf
This issu ... se pages are often still affected by injection issues, in which case there is still concern for
browser
At "High ... responses.

Solution:
Ensure t ... ppropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.
If possib ... nodern web browser that does not perform MIME-sniffing at all, or that can be directed by the
web app

Referenc
https://le ... xplorer/ie-developer/compatibility/gg622941(v=vs.85)
https://c

Alert Tag

	Value
CWE-69	https://cwe.mitre.org/data/definitions/693.html
OWASP_	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguratio...
POLICY_QA_STD	
POLICY_PENTEST	

Edit Alert

X-Content-Type-Options Header Missing

URL: http://localhost/DVWA/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%28%27XSS%27%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

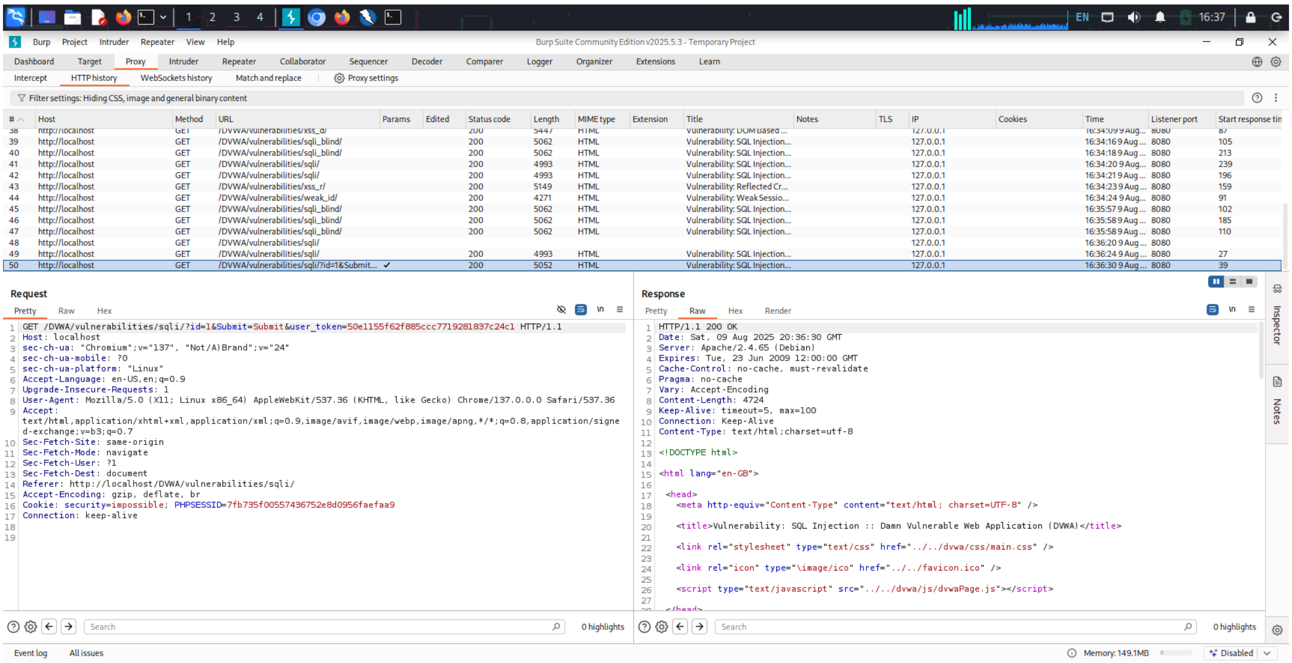
Alerts 🚩0 🚩2 🚩4 🚩4 Main Proxy: localhost:8081

Current Status 0 0 0 26 0 0 0 0 0 0

Future Interns - Task 1 Screenshots & Descriptions

Screenshot 4: Burp Suite SQL Injection Response

Burp Suite HTTP history showing SQL Injection exploitation returning database results.



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.3 - 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, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response tin
38	http://localhost	GET	/DVWA/vulnerabilities/xss_d/			200	5447	HTML		Vulnerability: DOM Based ...			127.0.0.1		16:34:09 9 Aug ...	8080	87
39	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:34:16 9 Aug ...	8080	105
40	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:34:18 9 Aug ...	8080	213
41	http://localhost	GET	/DVWA/vulnerabilities/sqli/			200	4993	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:34:20 9 Aug...	8080	239
42	http://localhost	GET	/DVWA/vulnerabilities/sqli/			200	4993	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:34:21 9 Aug ...	8080	196
43	http://localhost	GET	/DVWA/vulnerabilities/xss_r/			200	5149	HTML		Vulnerability: Reflected Cr...			127.0.0.1		16:34:23 9 Aug ...	8080	159
44	http://localhost	GET	/DVWA/vulnerabilities/weak_id/			200	4271	HTML		Vulnerability: Weak Sessio...			127.0.0.1		16:34:24 9 Aug...	8080	91
45	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:35:57 9 Aug ...	8080	102
46	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:35:58 9 Aug ...	8080	185
47	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:35:58 9 Aug ...	8080	110
48	http://localhost	GET	/DVWA/vulnerabilities/sqli/										127.0.0.1		16:36:20 9 Aug ...	8080	
49	http://localhost	GET	/DVWA/vulnerabilities/sqli/			200	4993	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:36:24 9 Aug ...	8080	27
50	http://localhost	GET	/DVWA/vulnerabilities/sqli/?id=1&Submit...	✓		200	5052	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:36:30 9 Aug ...	8080	39

Request

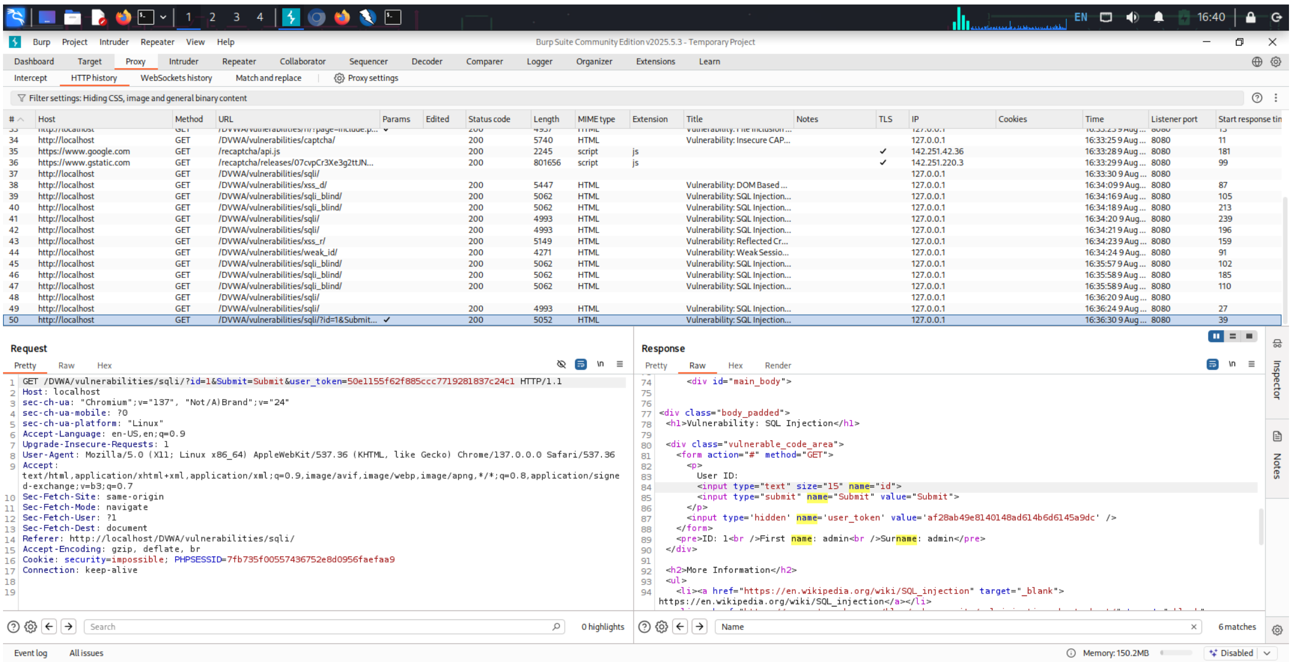
```
GET /DWWA/vulnerabilities/sqli/?id=1&Submit=Submit&user_token=50e1155f62f885ccc7719281837c24c1 HTTP/1.1
Host: localhost
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signe
d-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://localhost/DWWA/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=7fb735f00557436752e8d0956faefaa9
Connection: keep-alive
```

Response

```
HTTP/1.1 200 OK
Date: Sat, 09 Aug 2025 20:36:30 GMT
Server: Apache/2.4.65 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 4724
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8

<!DOCTYPE html>

<html lang="en-GB">

 <head>
   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

   <title>Vulnerability: SQL Injection :: Damn Vulnerable Web Application (DVWA)</title>

   <link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css" />

   <link rel="icon" type="\image/ico" href="../../favicon.ico" />

   <script type="text/javascript" src="../../dvwa/js/dvwaPage.js"></script>

 </head>
```

Screenshot 5: Burp Suite SQL Injection Proof

Detailed request and response demonstrating SQL Injection vulnerability in DVWA.



Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener port	Start response tim
34	http://localhost	GET	/DVWA/vulnerabilities/captcha/			200	5740	HTML		Vulnerability: Insecure CAP...			127.0.0.1		16:33:25 9 Aug ...	8080	11
35	https://www.google.com	GET	/recaptcha/api.js			200	2245	script	js			✓	142.251.42.36		16:33:28 9 Aug ...	8080	181
36	https://www.gstatic.com	GET	/recaptcha/releases/07cvpCr3Xe3g2ttJN...			200	801656	script	js			✓	142.251.220.3		16:33:29 9 Aug ...	8080	99
37	http://localhost	GET	/DVWA/vulnerabilities/sqli/										127.0.0.1		16:33:30 9 Aug ...	8080	
38	http://localhost	GET	/DVWA/vulnerabilities/xss_d/			200	5447	HTML		Vulnerability: DOM Based ...			127.0.0.1		16:34:09 9 Aug...	8080	87
39	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:34:16 9 Aug ...	8080	105
40	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:34:18 9 Aug ...	8080	213
41	http://localhost	GET	/DVWA/vulnerabilities/sqli/			200	4993	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:34:20 9 Aug...	8080	239
42	http://localhost	GET	/DVWA/vulnerabilities/sqli/			200	4993	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:34:21 9 Aug ...	8080	196
43	http://localhost	GET	/DVWA/vulnerabilities/xss_r/			200	5149	HTML		Vulnerability: Reflected Cr...			127.0.0.1		16:34:23 9 Aug ...	8080	159
44	http://localhost	GET	/DVWA/vulnerabilities/weak_id/			200	4271	HTML		Vulnerability: Weak Sessio...			127.0.0.1		16:34:24 9 Aug...	8080	91
45	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:35:57 9 Aug ...	8080	102
46	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:35:58 9 Aug ...	8080	185
47	http://localhost	GET	/DVWA/vulnerabilities/sqli_blind/			200	5062	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:35:58 9 Aug ...	8080	110
48	http://localhost	GET	/DVWA/vulnerabilities/sqli/										127.0.0.1		16:36:20 9 Aug ...	8080	
49	http://localhost	GET	/DVWA/vulnerabilities/sqli/			200	4993	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:36:24 9 Aug ...	8080	27
50	http://localhost	GET	/DVWA/vulnerabilities/sqli/?id=1&Submit...	✓		200	5052	HTML		Vulnerability: SQL Injection...			127.0.0.1		16:36:30 9 Aug ...	8080	39

Request

```
GET /DVWA/vulnerabilities/sqli/?id=1&Submit=Submit&user_token=50e1155f62f885ccc7719281837c24c1 HTTP/1.1
Host: localhost
sec-ch-ua: "Chromium";v="137", "Not/A)Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signe
d-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://localhost/DVWA/vulnerabilities/sqli/
Accept-Encoding: gzip, deflate, br
Cookie: security=impossible; PHPSESSID=7fb735f00557436752e8d0956faefaa9
Connection: keep-alive


```

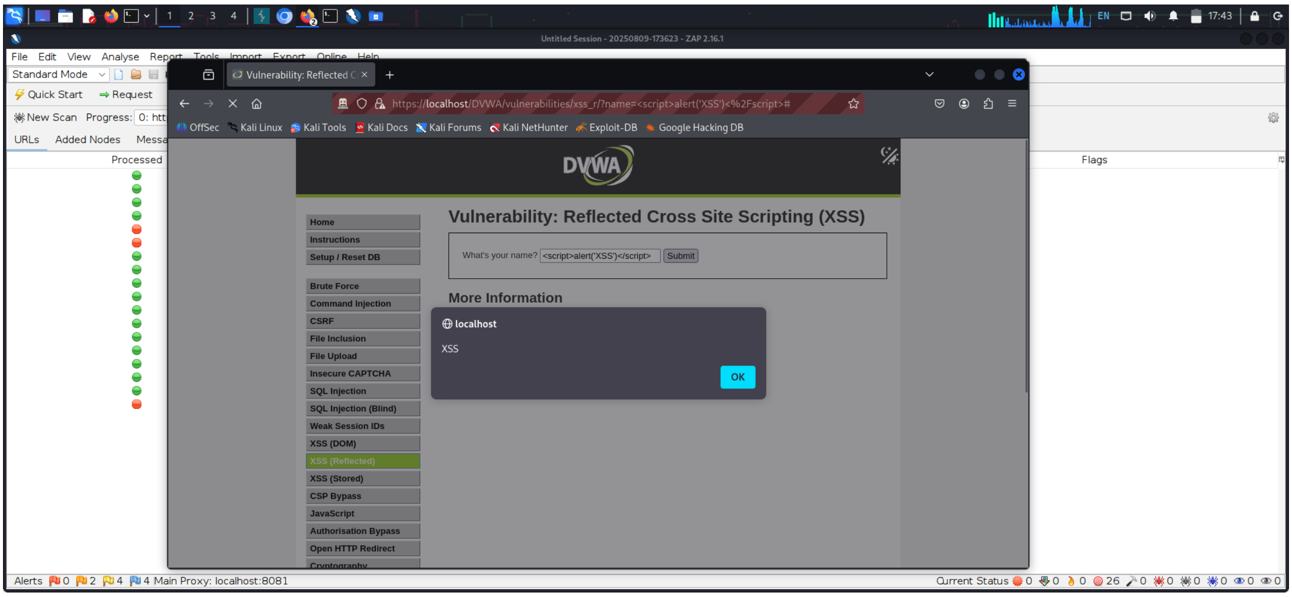
Response

```
      <div id="main_body">


<div class="body_padded">
  <h1>Vulnerability: SQL Injection</h1>

  <div class="vulnerable_code_area">
    <form action="#" method="GET">
      <p>
        User ID:
        <input type="text" size="15" name="id">
        <input type="submit" name="Submit" value="Submit">
      </p>
      <input type='hidden' name='user_token' value='af28ab49e8140148ad614b6d6145a9dc' />
    </form>
    <pre>ID: 1<br />First name: admin<br />Surname: admin</pre>
  </div>

  <h2>More Information</h2>
  <ul>
    <li><a href="https://en.wikipedia.org/wiki/SQL_injection" target="_blank">
https://en.wikipedia.org/wiki/SQL_injection</a></li>
```

Future Interns - Task 1 Screenshots & Descriptions

Screenshot 7: XSS Proof of Concept

Reflected Cross-Site Scripting executed in DVWA, triggering a JavaScript alert box.



Untitled Session - 20250809-173623 - ZAP 2.16.1

https://localhost/DVWA/vulnerabilities/xss_r/?name=<script>alert('XSS')<%2Fscript>#

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? <script>alert('XSS')</script>

More Information

localhost

XSS

Alerts 0 2 4 4 Main Proxy: localhost:8081

Current Status 0 0 0 26 0 0 0 0 0 0