Experiment No. 8

Title: Working with Burp

Roll No.: 16010423076 **Experiments No.:8**

Aim :To use Burp Suite for intercepting, modifying, and testing web application security.

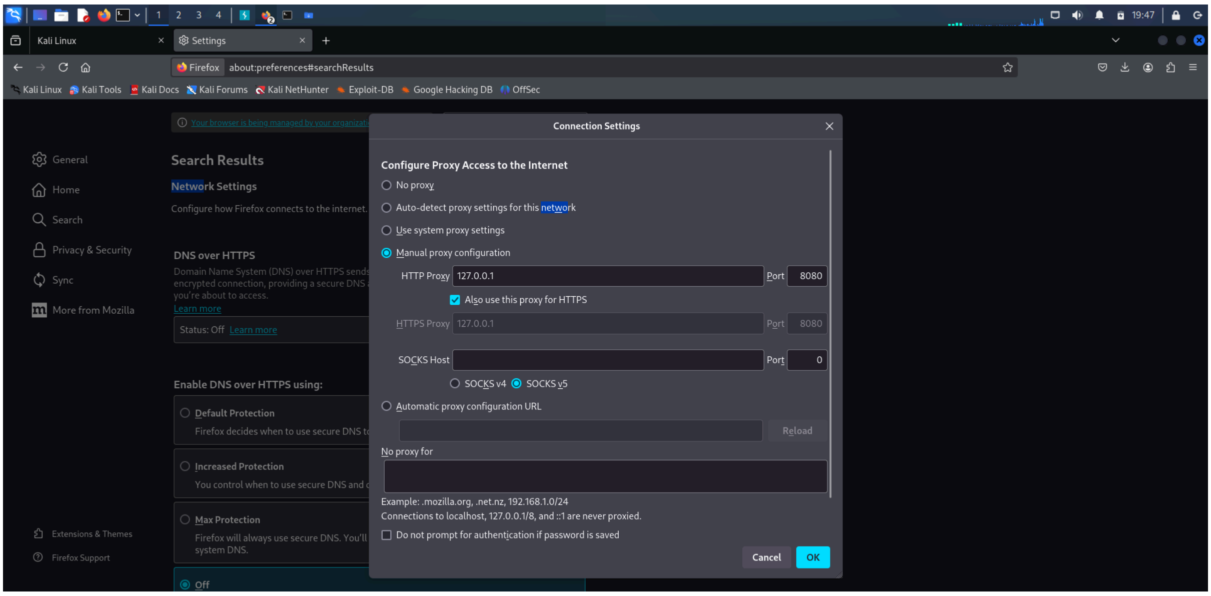
Resources : Linux Machine, Internet, Browser

Theory:
Burp Suite is an essential tool for web security testing. It provides functionalities such as intercepting requests, modifying parameters, and performing security scans. This experiment focuses on active testing, including altering requests, performing a passive scan, testing for Cross-Site Scripting (XSS), and simulating weak authentication attacks using Burp Intruder. These techniques help identify vulnerabilities in web applications and strengthen their security.

IMPLEMENTATION AND RESULTS:

1. Configure Firefox to Use Burp Proxy

- Set HTTP Proxy to 127.0.0.1 and Port to 8080.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy
○ Auto-detect proxy settings for this network
○ Use system proxy settings
● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Also use this proxy for HTTPS

HTTPS Proxy 127.0.0.1 Port 8080

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

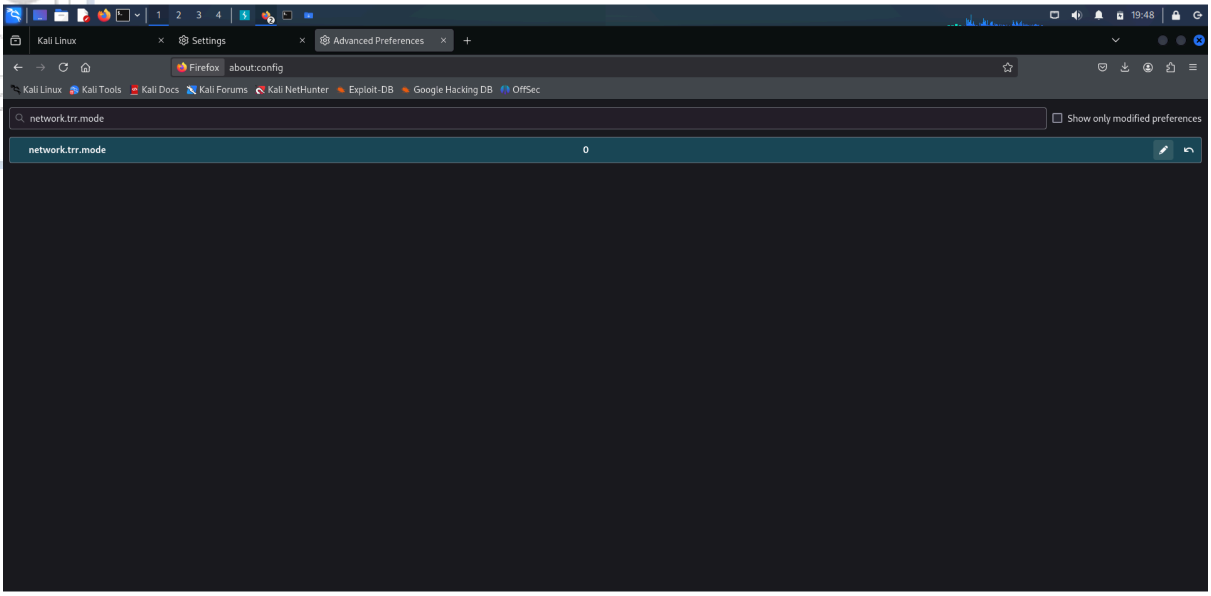
Reload

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24
Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

□ Do not prompt for authentication if password is saved

Cancel OK

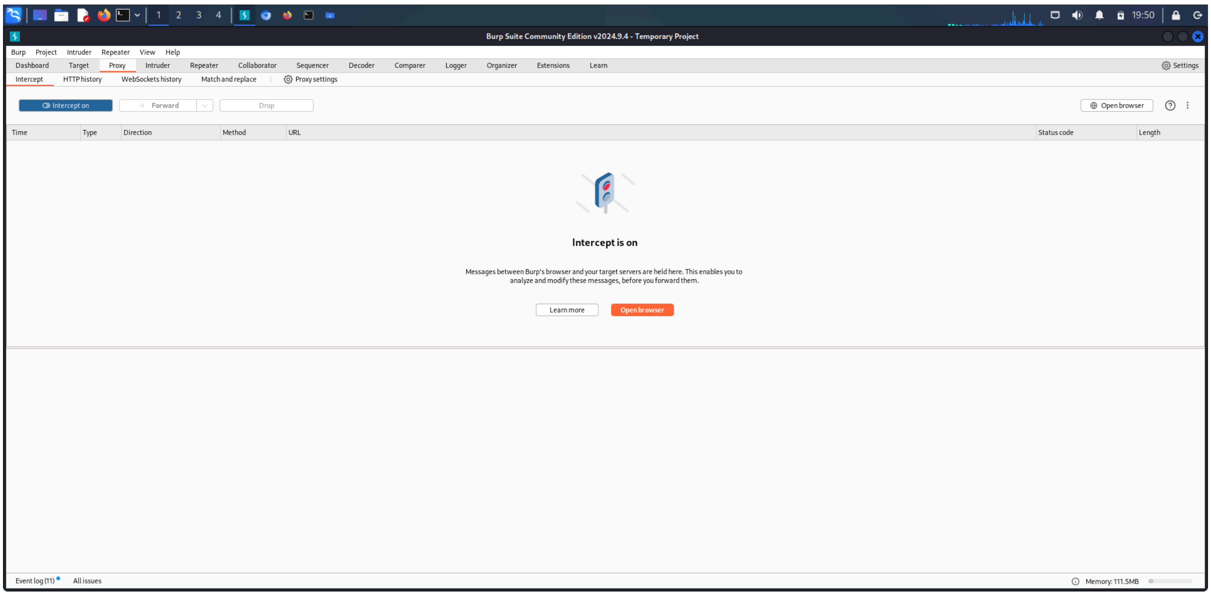

Kali Linux
Settings
Advanced Preferences
Firefox about:config
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Show only modified preferences

network.trr.mode

network.trr.mode 0

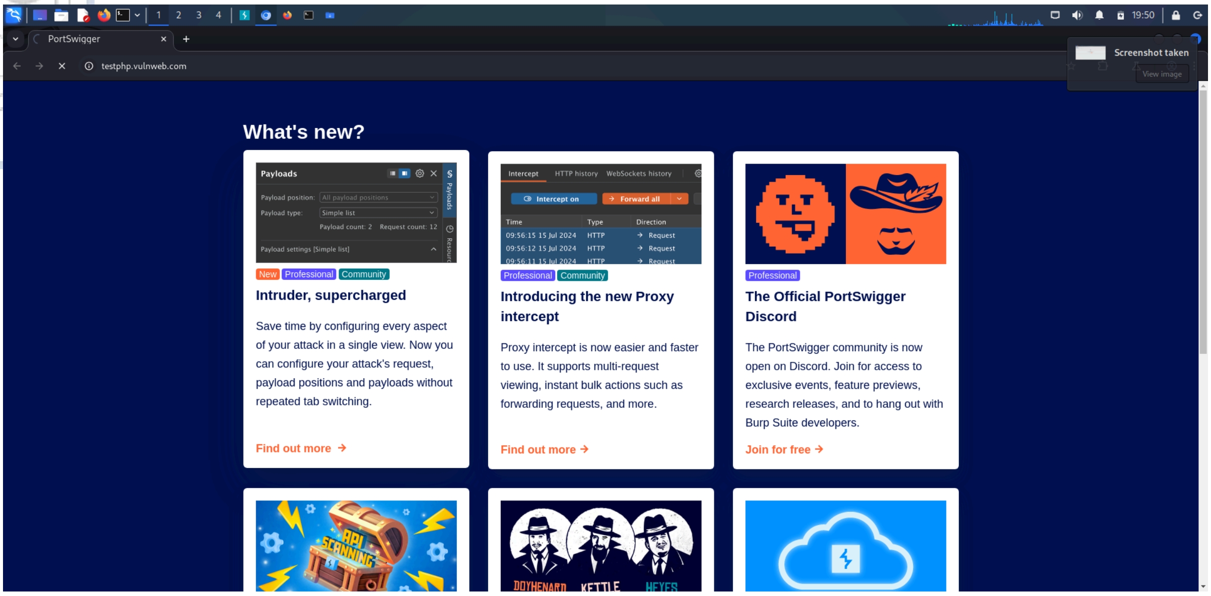
2. Verify Interception Works

- Open Firefox and visit http://testphp.vulnweb.com/.
- You should see a request intercepted in Burp Suite.


Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Time Type Direction Method URL Status code Length
Learn more
Open browser
Event log (11) All issues
Memory: 111.5MB

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.



What's new?

New Professional Community

Intruder, supercharged

Save time by configuring every aspect of your attack in a single view. Now you can configure your attack's request, payload positions and payloads without repeated tab switching.

Find out more →

Professional Community

Introducing the new Proxy intercept

Proxy intercept is now easier and faster to use. It supports multi-request viewing, instant bulk actions such as forwarding requests, and more.

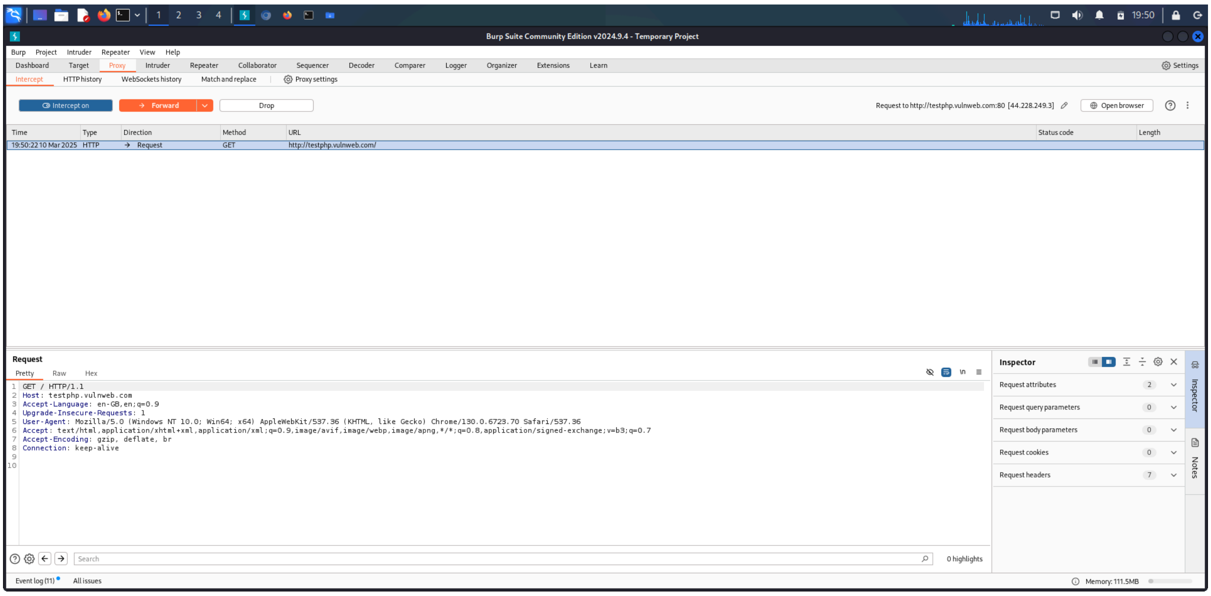
Find out more →

Professional

The Official PortSwigger Discord

The PortSwigger community is now open on Discord. Join for access to exclusive events, feature previews, research releases, and to hang out with Burp Suite developers.

Join for free →



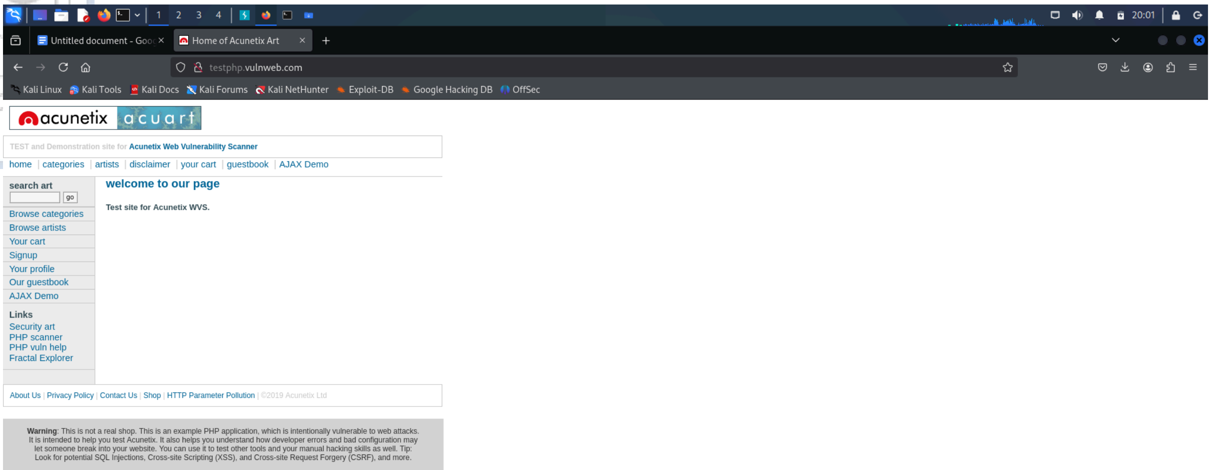
Request to http://testphp.vulnweb.com:80 [44.228.249.3]

Time	Type	Direction	Method	URL	Status code	Length
19:50:22 10 Mar 2025	HTTP	→ Request	GET	http://testphp.vulnweb.com/		

Request

Pretty Raw Hex

```
GET / HTTP/1.1
Host: testphp.vulnweb.com
Accept-Language: en-GB,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 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
Accept-Encoding: gzip, deflate, br
Connection: keep-alive


```



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

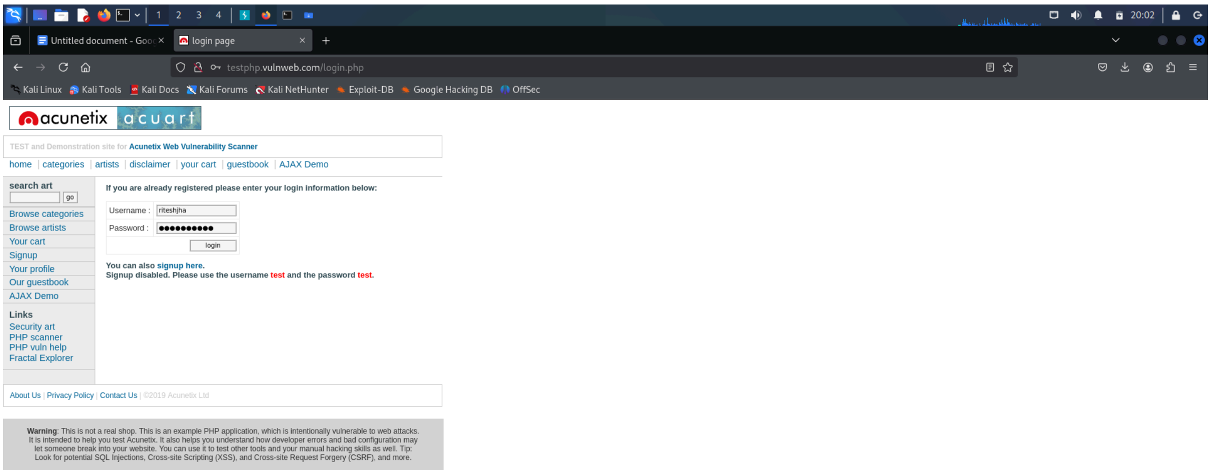
welcome to our page

Test site for Acunetix WVS.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

3. Intercept and Modify a Request

- Try to log in with random credentials.
- The request will be intercepted → Modify the request



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

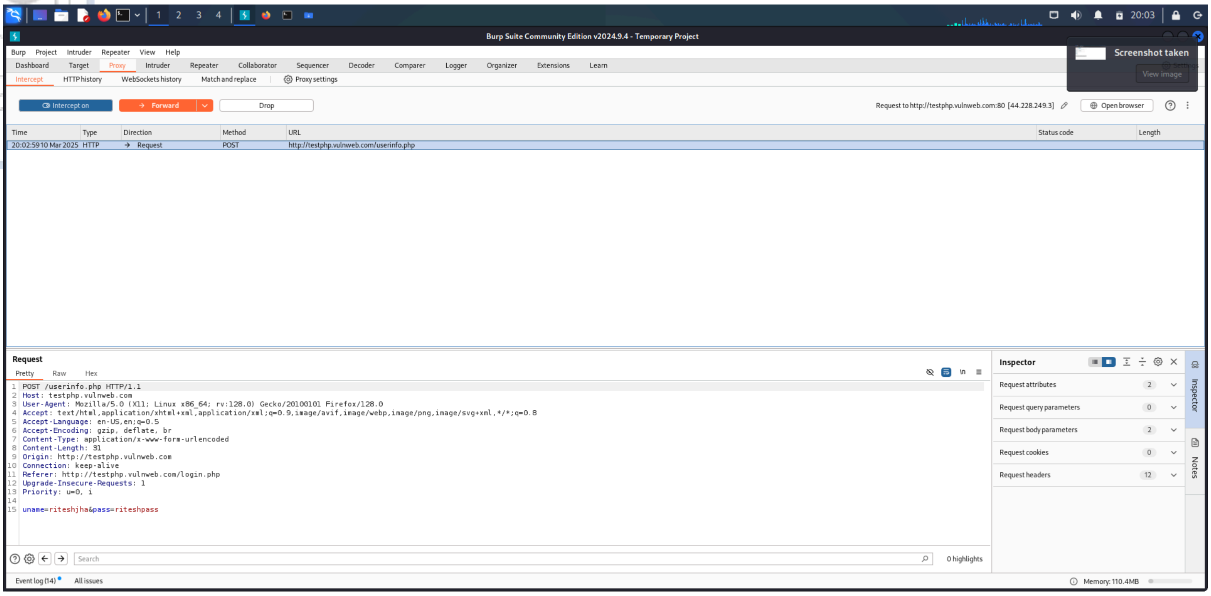
If you are already registered please enter your login information below:

Username : riteshjha

Password : ●●●●●●●●●●●

You can also signup here.
Signup disabled. Please use the username test and the password test.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

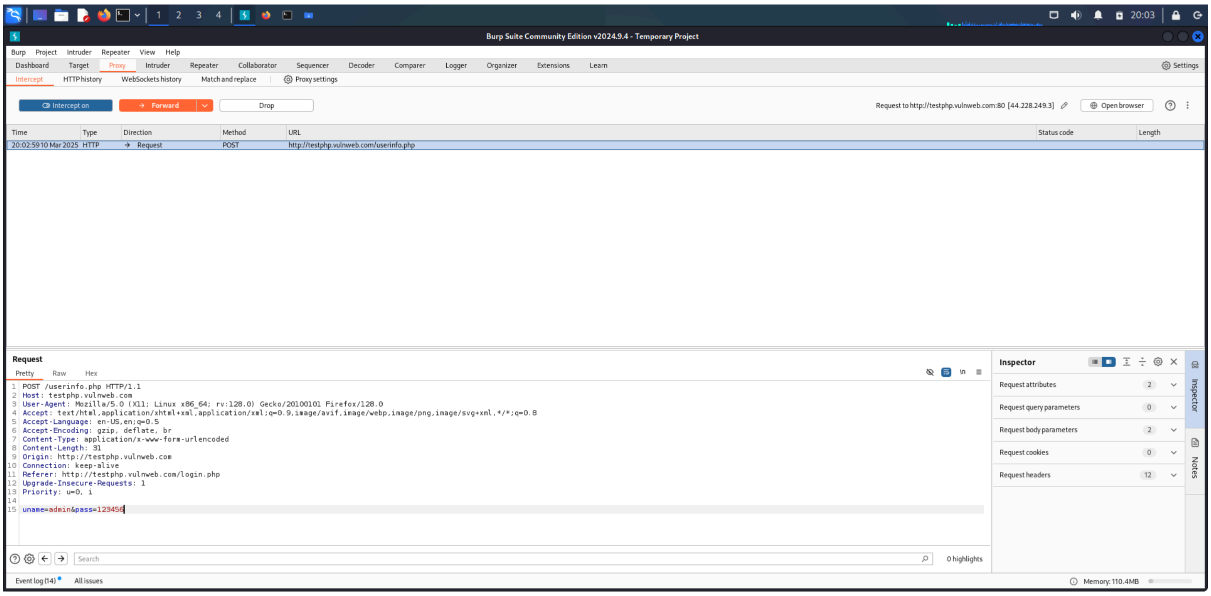


Request to http://testphp.vulnweb.com:80 [44.228.249.3]

Time	Type	Direction	Method	URL	Status code	Length
20:02:59 10 Mar 2025	HTTP	→ Request	POST	http://testphp.vulnweb.com/userinfo.php		

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

uname=riteshjha&pass=riteshpass
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	2
Request cookies	0
Request headers	12



Request to http://testphp.vulnweb.com:80 [44.228.249.3]

Time	Type	Direction	Method	URL	Status code	Length
20:02:59 10 Mar 2025	HTTP	→ Request	POST	http://testphp.vulnweb.com/userinfo.php		

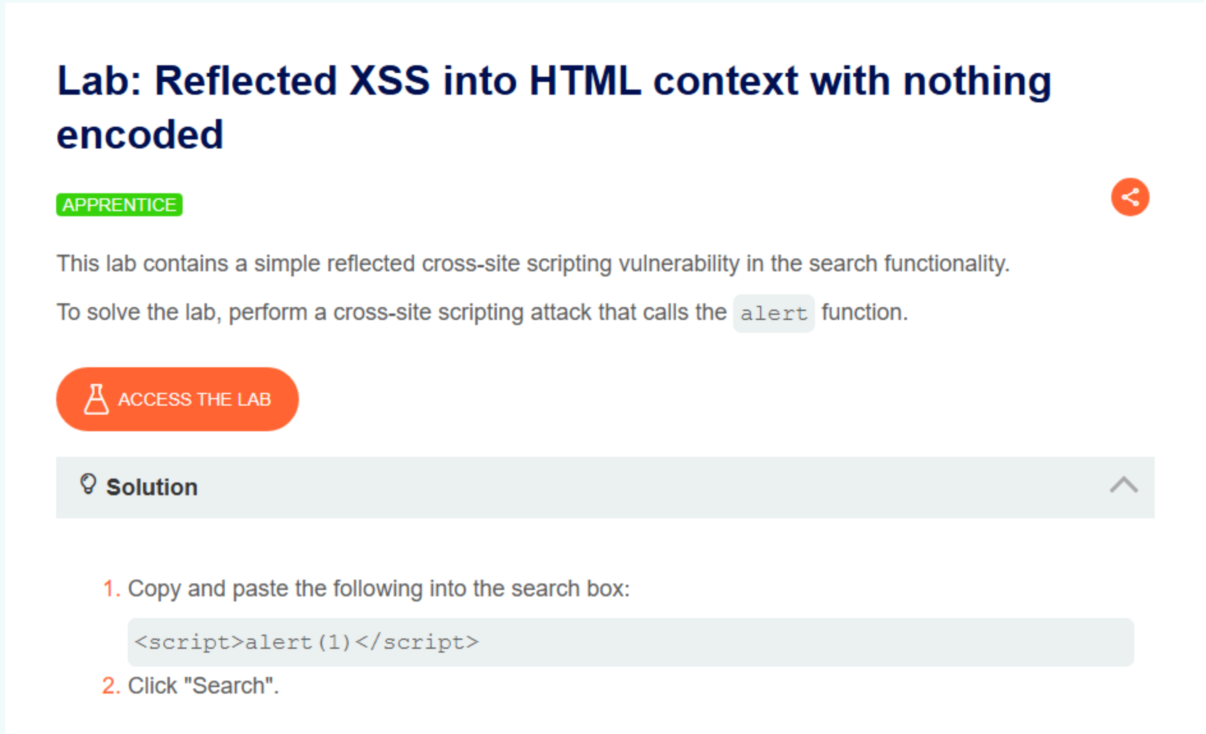
```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 31
Origin: http://testphp.vulnweb.com
Connection: keep-alive
Referer: http://testphp.vulnweb.com/login.php
Upgrade-Insecure-Requests: 1
Priority: u=0, i

uname=admin&pass=123456
```

Inspector	
Request attributes	2
Request query parameters	0
Request body parameters	2
Request cookies	0
Request headers	12

4. Test for XSS Vulnerabilities

- Find a search box or form input.
- Enter <script>alert("XSS")</script> and submit.

Lab 1



Lab: Reflected XSS into HTML context with nothing encoded

APPRENTICE

This lab contains a simple reflected cross-site scripting vulnerability in the search functionality.

To solve the lab, perform a cross-site scripting attack that calls the `alert` function.

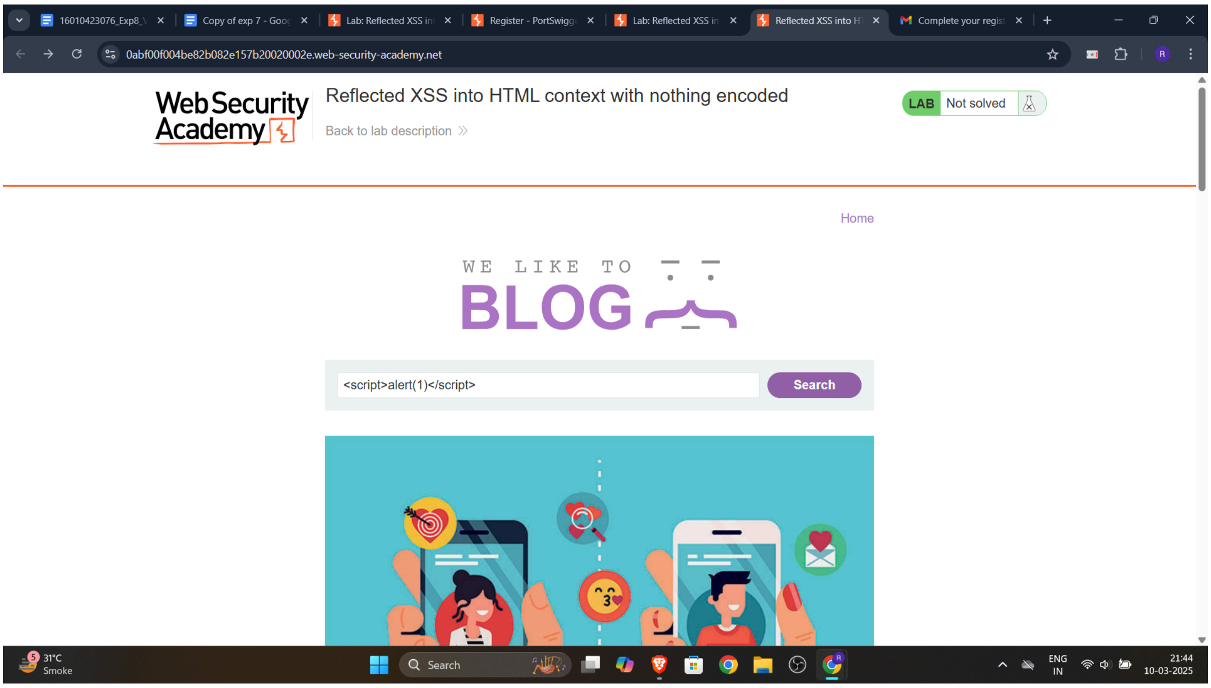
ACCESS THE LAB

Solution

1. Copy and paste the following into the search box:

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

2. Click "Search".



Web Security Academy

Reflected XSS into HTML context with nothing encoded

Back to lab description »

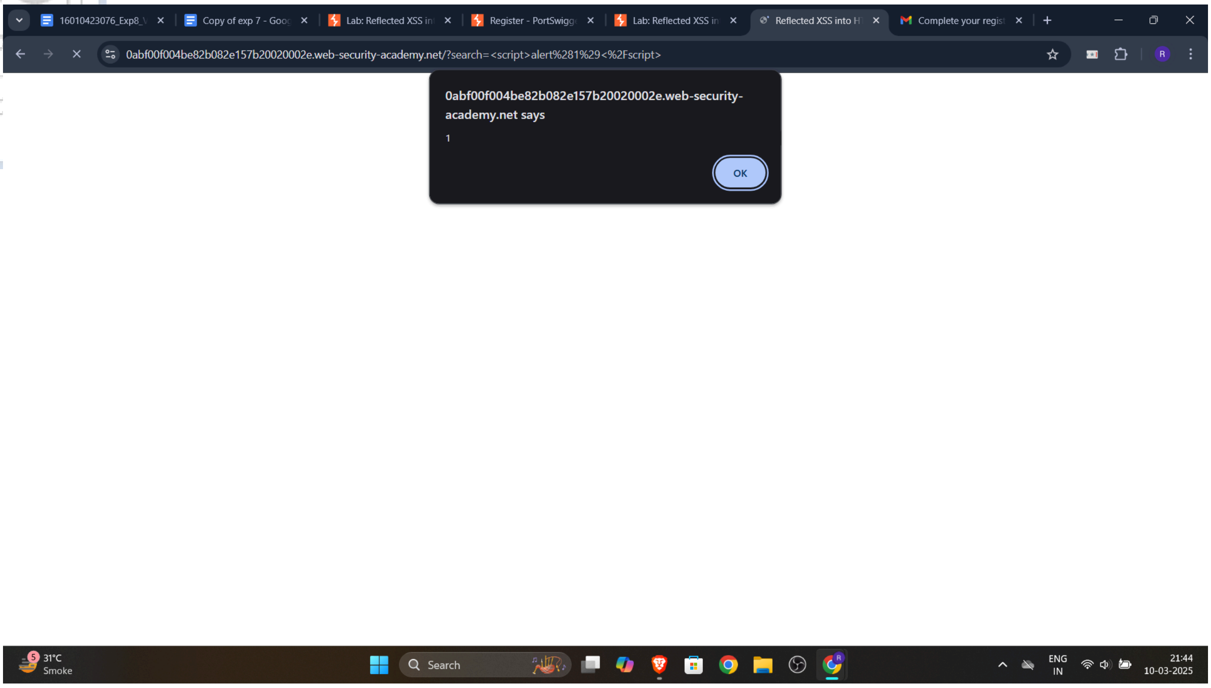
LAB Not solved

Home

WE LIKE TO BLOG

<script>alert(1)</script>

Search



0abf00f004be82b082e157b20020002e.web-security-academy.net/?search=<script>alert%281%29<%2Fscript>

0abf00f004be82b082e157b20020002e.web-security-academy.net says

1

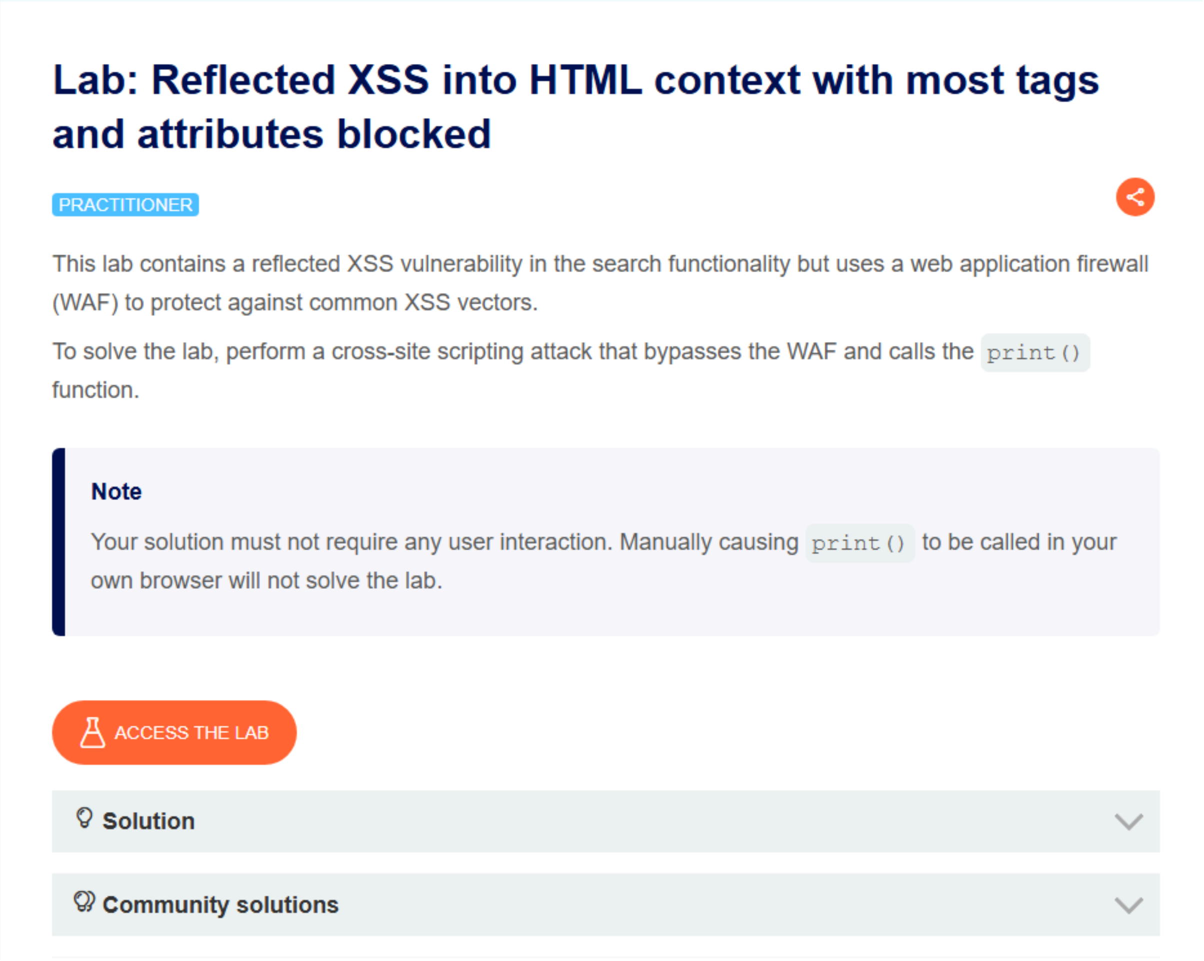
Lab 2

Step 1: Try a Basic XSS Payload

Step 2: Find Allowed HTML Tags using Burp Intruder

Step 3: Find Allowed Event Handlers

Step 4: Create the Final XSS Payload



Lab: Reflected XSS into HTML context with most tags and attributes blocked

PRACTITIONER

This lab contains a reflected XSS vulnerability in the search functionality but uses a web application firewall (WAF) to protect against common XSS vectors.

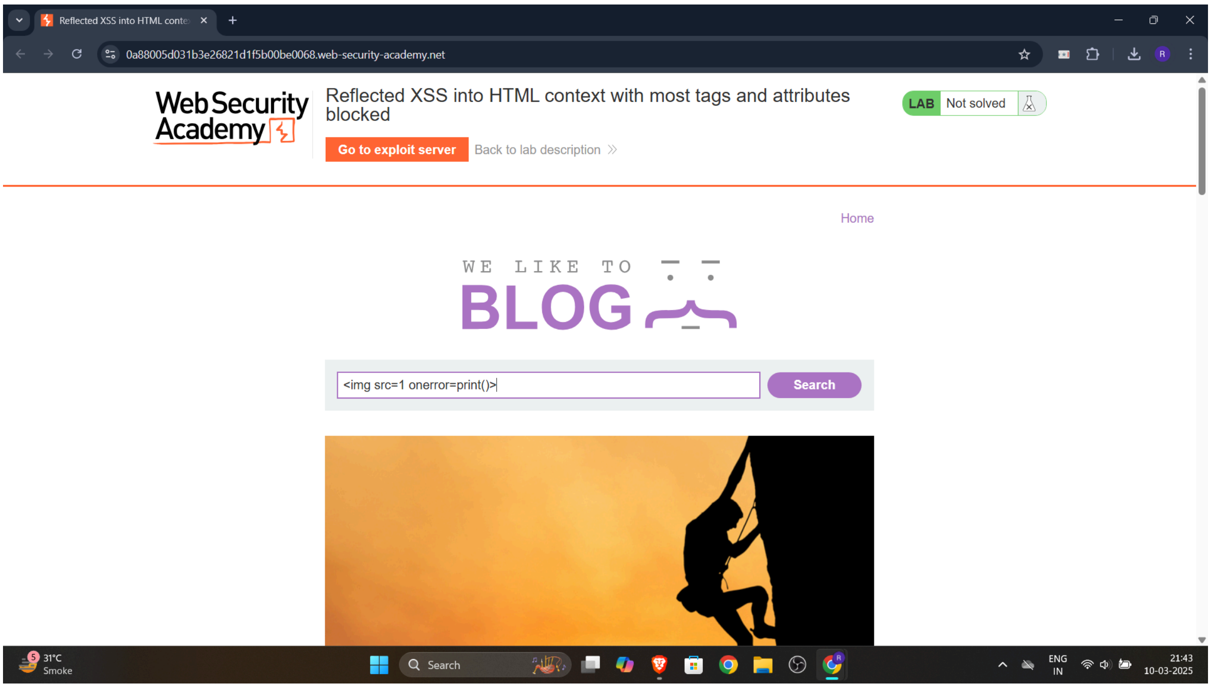
To solve the lab, perform a cross-site scripting attack that bypasses the WAF and calls the `print()` function.

> **Note**
>
> Your solution must not require any user interaction. Manually causing `print()` to be called in your own browser will not solve the lab.

ACCESS THE LAB

Solution

Community solutions



Reflected XSS into HTML conte...

0a88005d031b3e26821d1f5b00be0068.web-security-academy.net

Web Security Academy

Reflected XSS into HTML context with most tags and attributes blocked

LAB Not solved

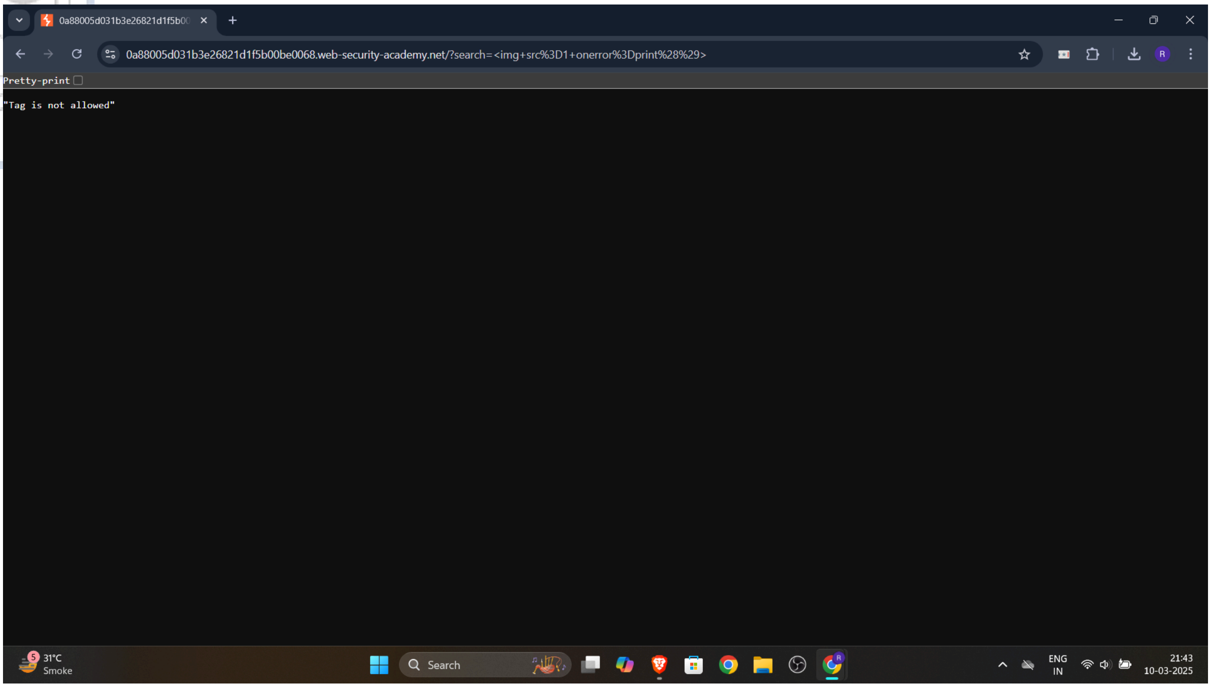
Go to exploit server Back to lab description »

Home

WE LIKE TO BLOG

```
<img src=1 onerror=print()>
```

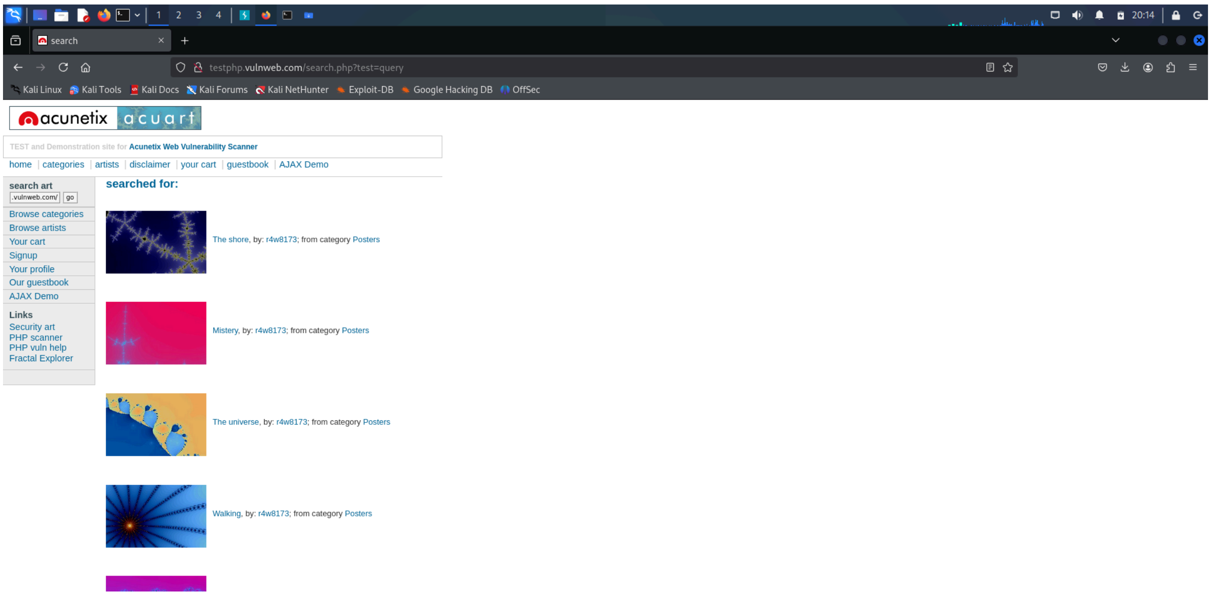
Search



```
0a88005d031b3e26821d1f5b00be0068.web-security-academy.net/?search=<img+src%3D1+onerror%3Dprint%28%29>
```

Pretty-print □

```
"Tag is not allowed"
```



```
testphp.vulnweb.com/search.php?test=query
```

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

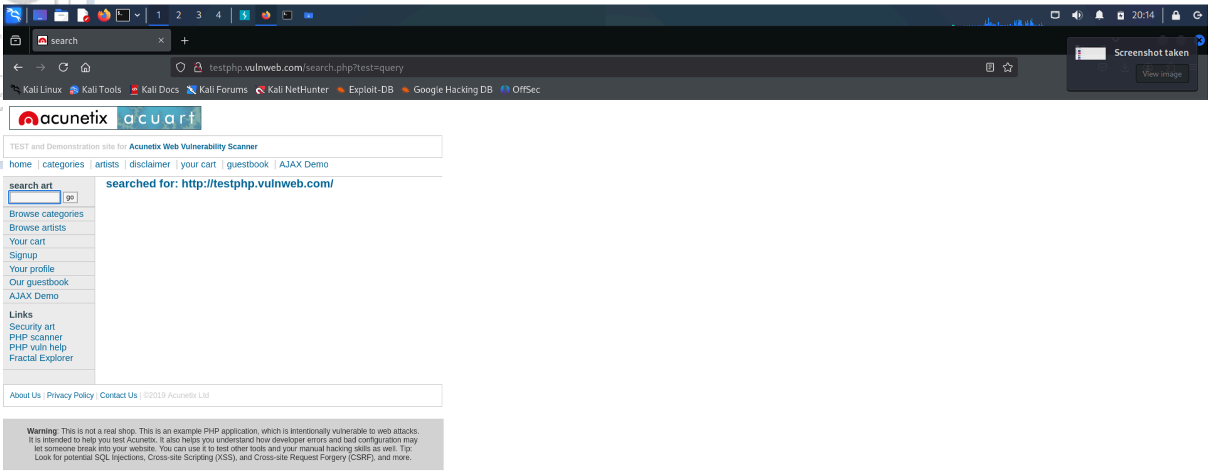
searched for:

The shore, by: r4w8173; from category Posters

Mistery, by: r4w8173; from category Posters

The universe, by: r4w8173; from category Posters

Walking, by: r4w8173; from category Posters



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

searched for: http://testphp.vulnweb.com/

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

Outcomes: CO3: Understand attack methodology

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

From this experiment, I learned how to actively test web applications using Burp Suite. By intercepting and modifying HTTP requests, scanning websites, and attempting authentication bypass, I understood how attackers exploit vulnerabilities. This experiment provided hands-on experience in ethical hacking techniques and reinforced the importance of securing web applications against common attacks.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

https://portswigger.net/burp/documentation

https://www.mozilla.org/en-US/firefox/new/

http://testphp.vulnweb.com