Lab Experiment: 6 Finding & Exploiting XSS Vulnerabilities using DVWA on Kali Linux

HARI VIGNESH RAO 23BD1A052Q

Aim

To identify and exploit Cross-Site Scripting (XSS) vulnerabilities in a vulnerable web application (DVWA) using Kali Linux.

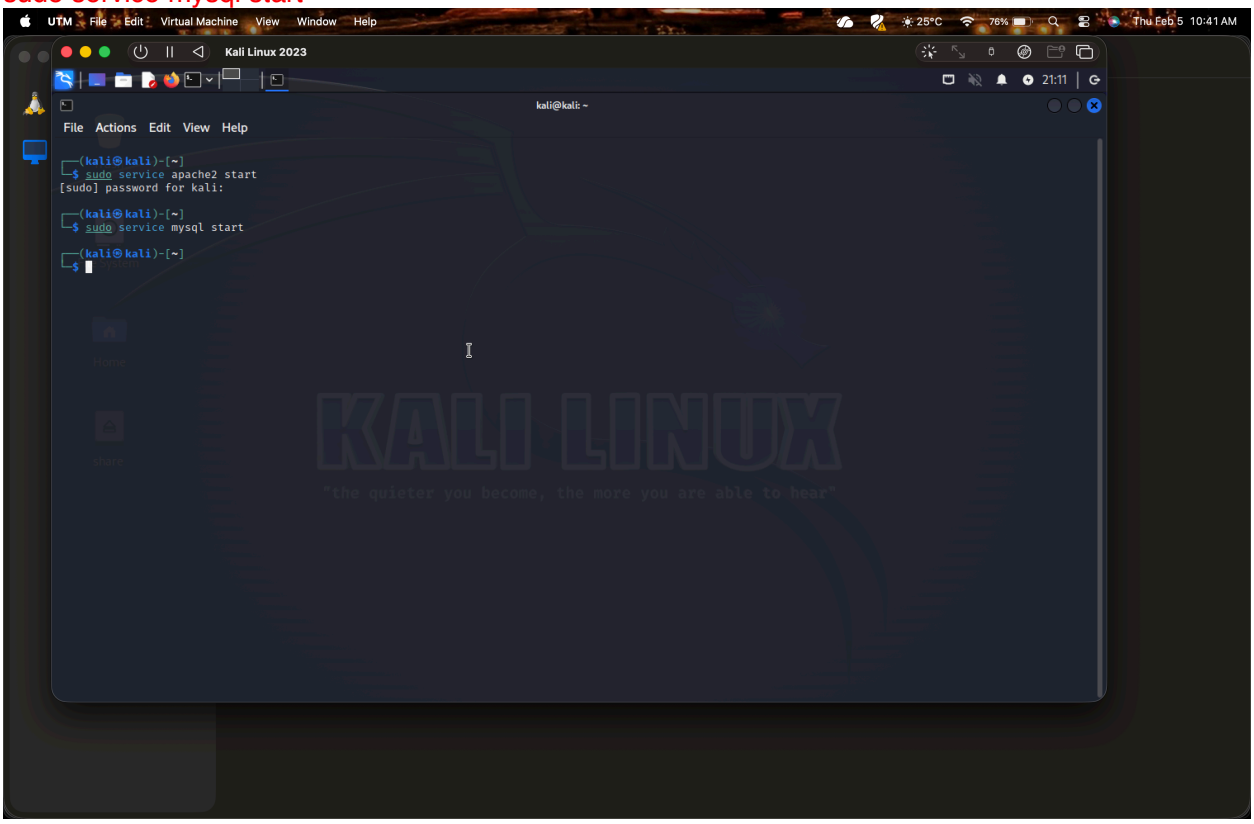
Requirements

- Kali Linux
- DVWA (Damn Vulnerable Web Application)
- Browser (Firefox/Chromium)
- Apache & MySQL running

Step 1: Start DVWA Services

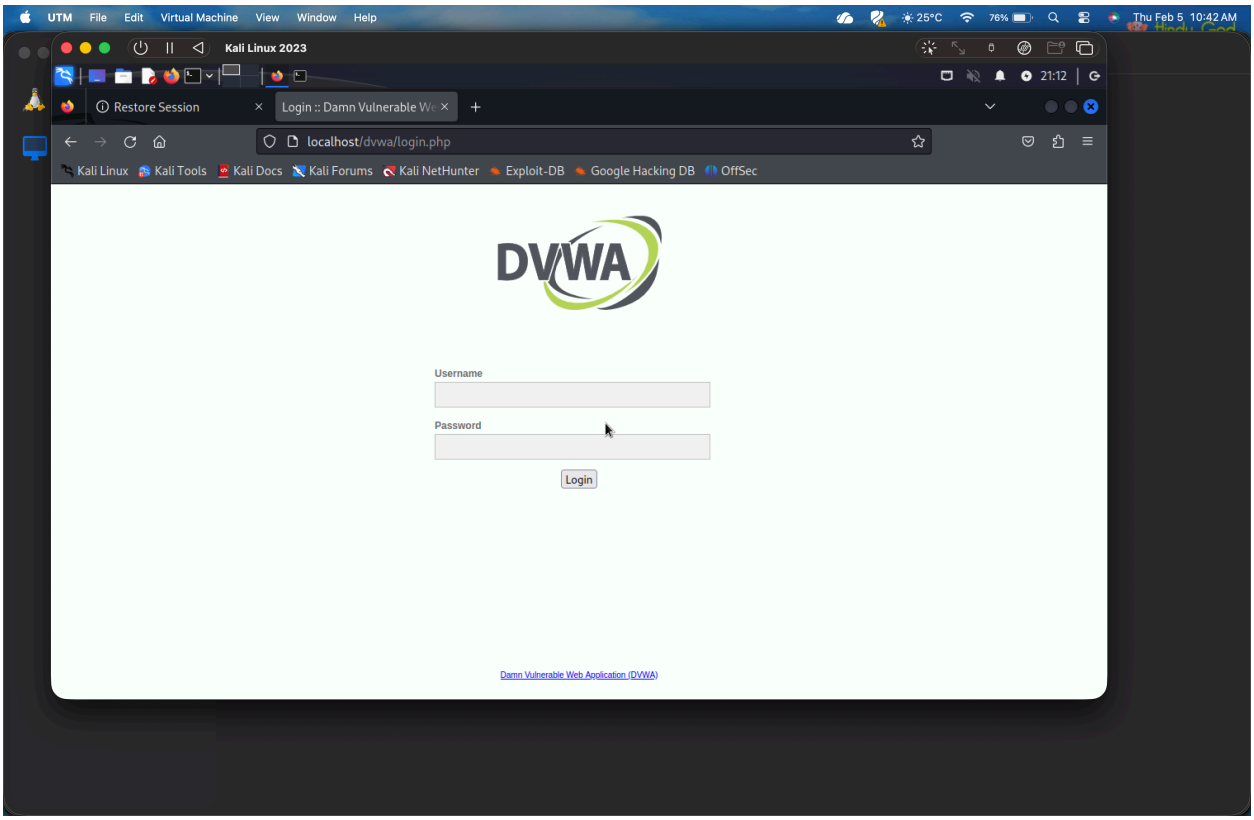
Open terminal:

```
sudo service apache2 start
sudo service mysql start
```



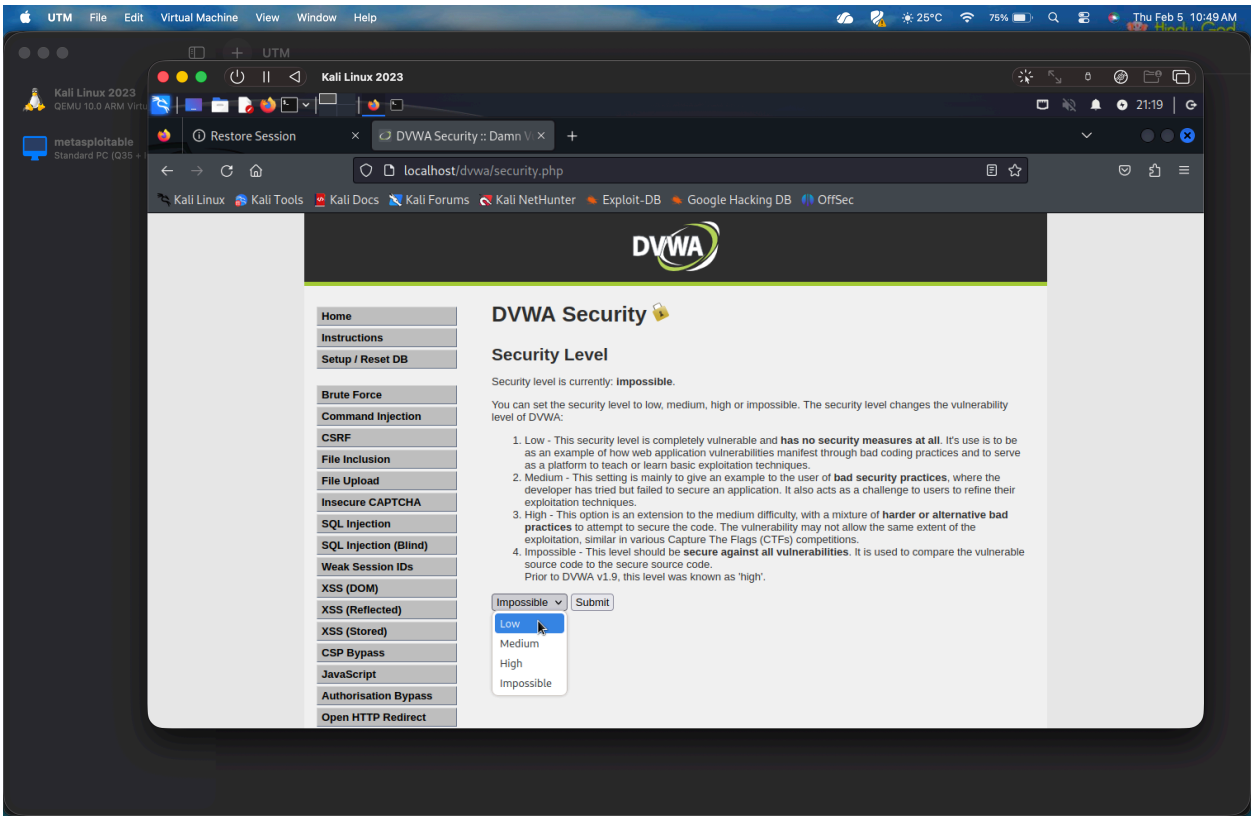
Open browser and go to:

http://localhost/dvwa

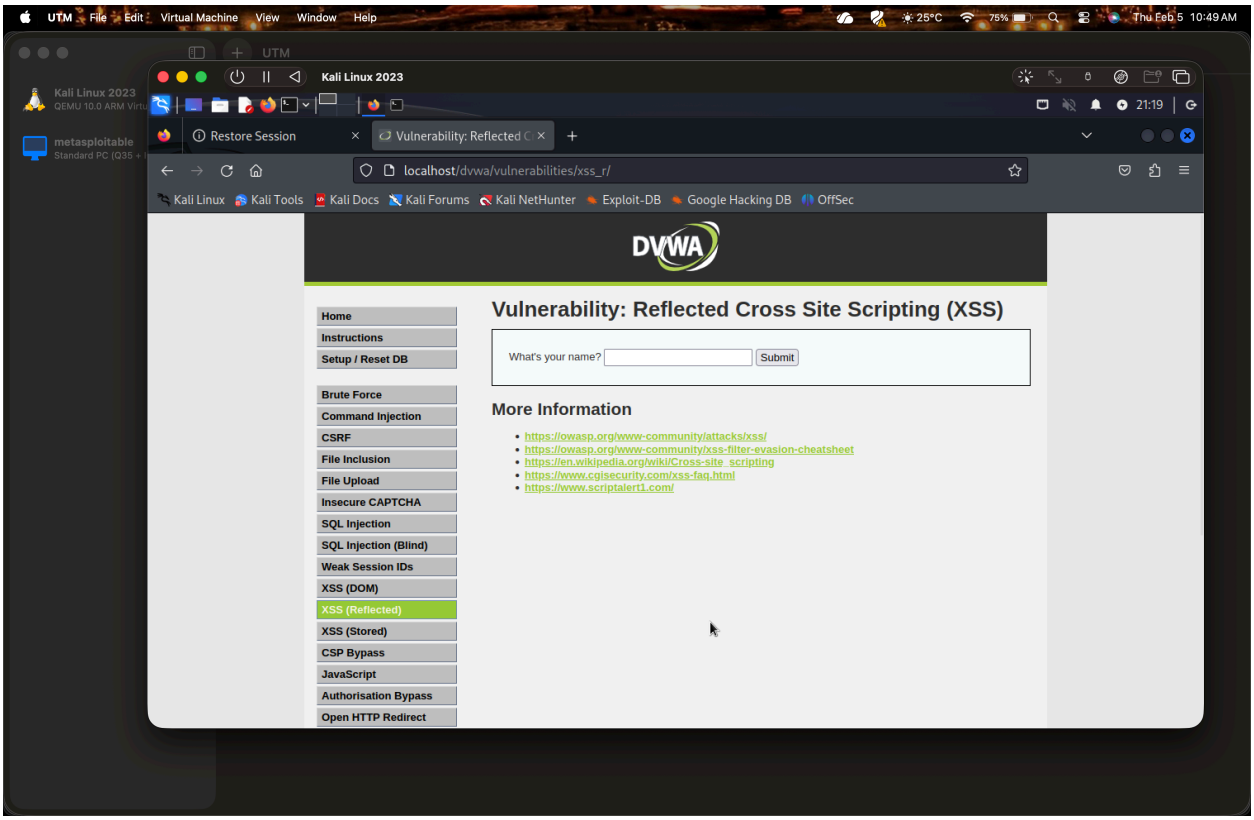


Login:

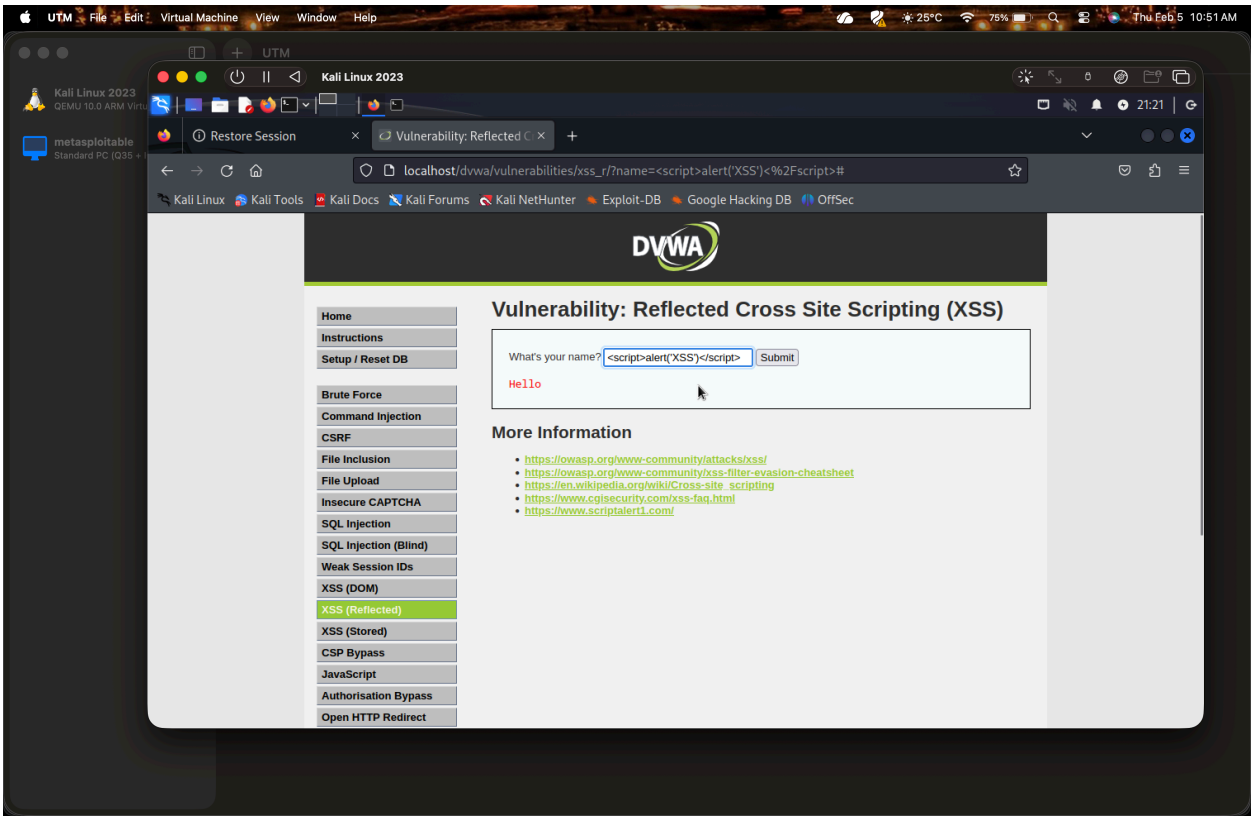
- Username: admin
- Password: passwordClick DVWA Security → set level to Low → Submit.



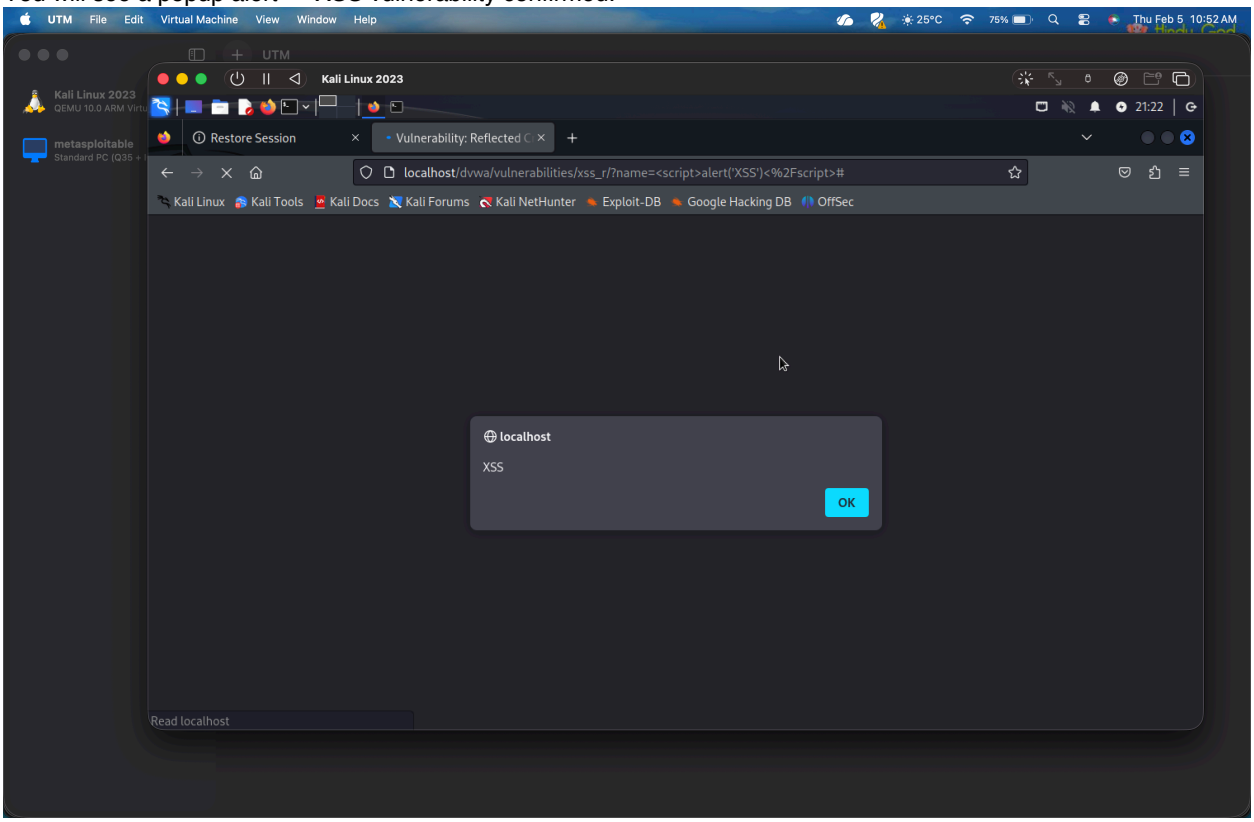
Step 2: Understanding XSS
XSS allows attackers to inject JavaScript code into a webpage that runs in another user's browser.
Types in DVWA:
• Reflected XSS
• Stored XSS
• DOM Based XSS
Step 3: Reflected XSS Test
Go to:
DVWA → XSS (Reflected)



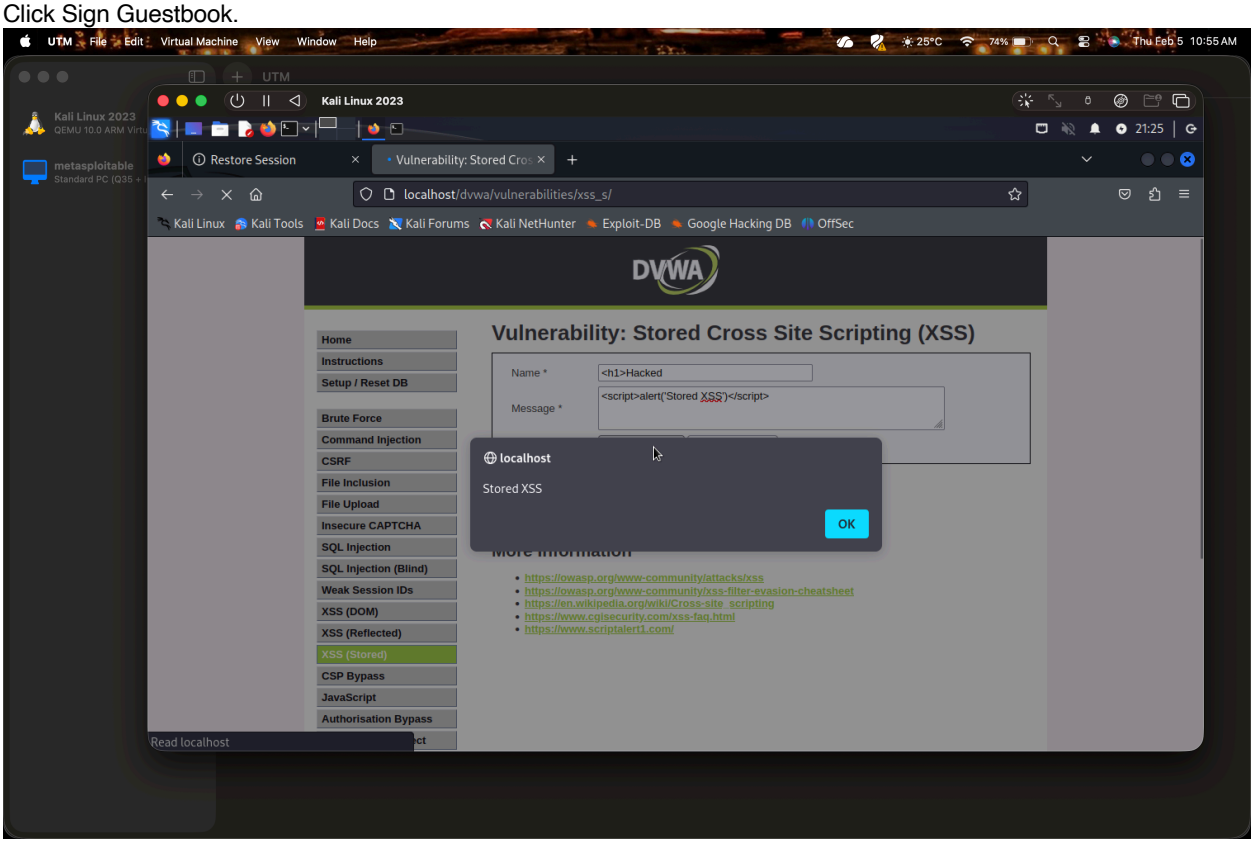
In the input box, type:
<script>alert('XSS')</script>
Click Submit.



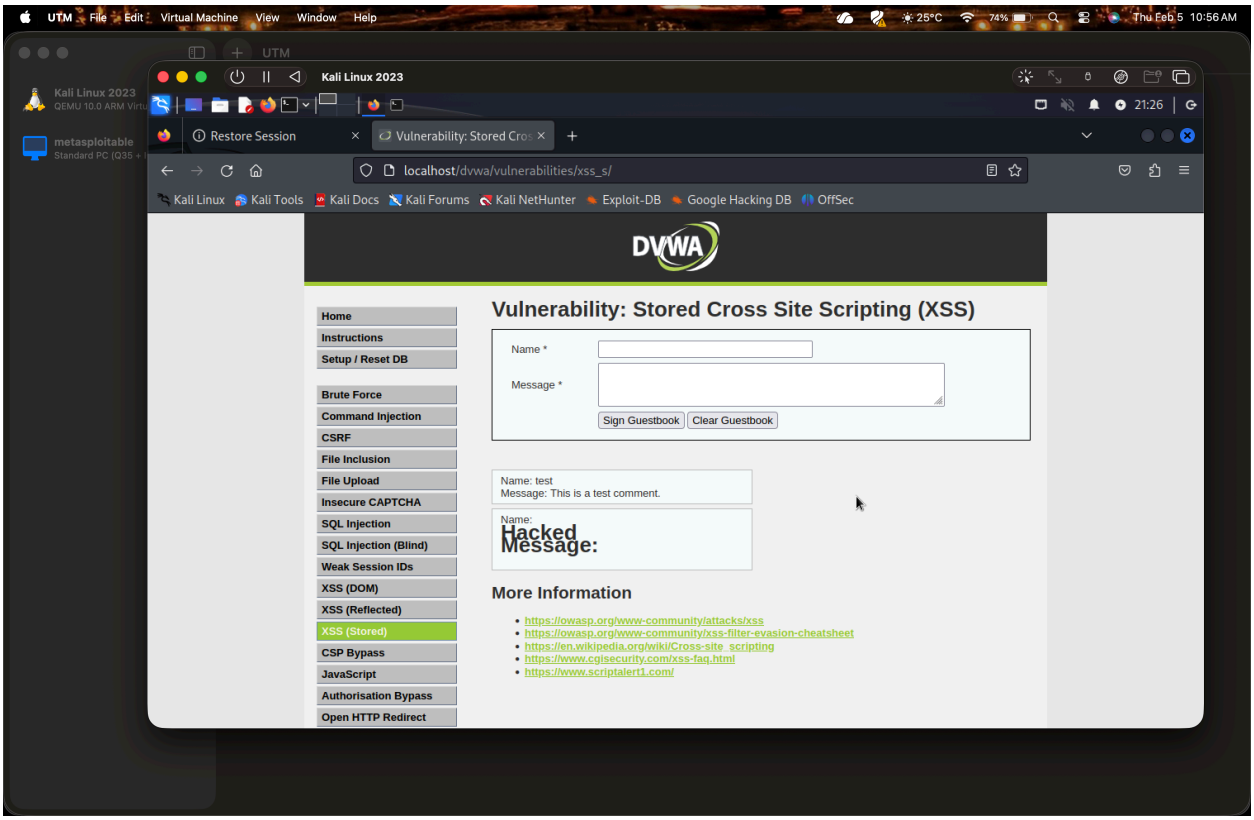
Output:
You will see a popup alert → XSS vulnerability confirmed.



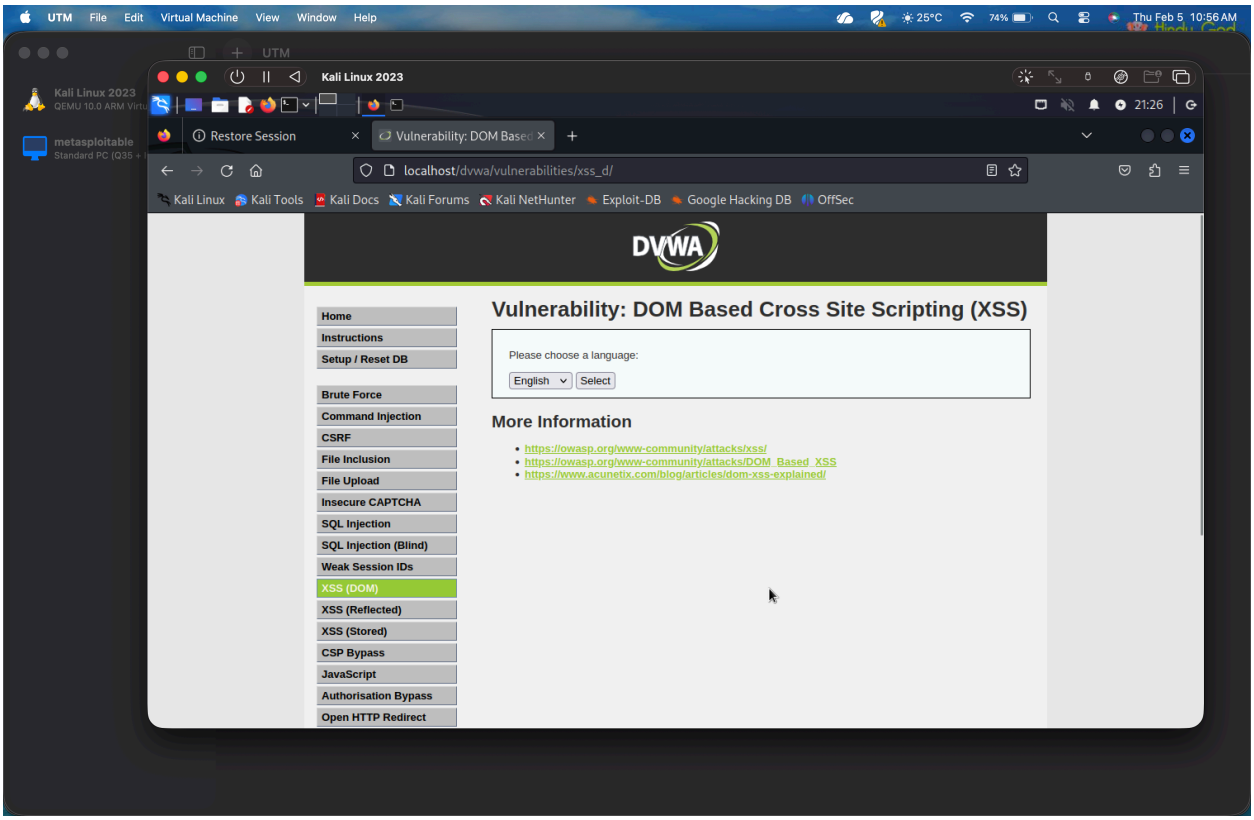
Step 4: Stored XSS Test
Go to:
DVWA → XSS (Stored)
Fill the form:
Name:
<h1>Hacked</h1>
Message:
<script>alert('Stored XSS')</script>
Click Sign Guestbook.



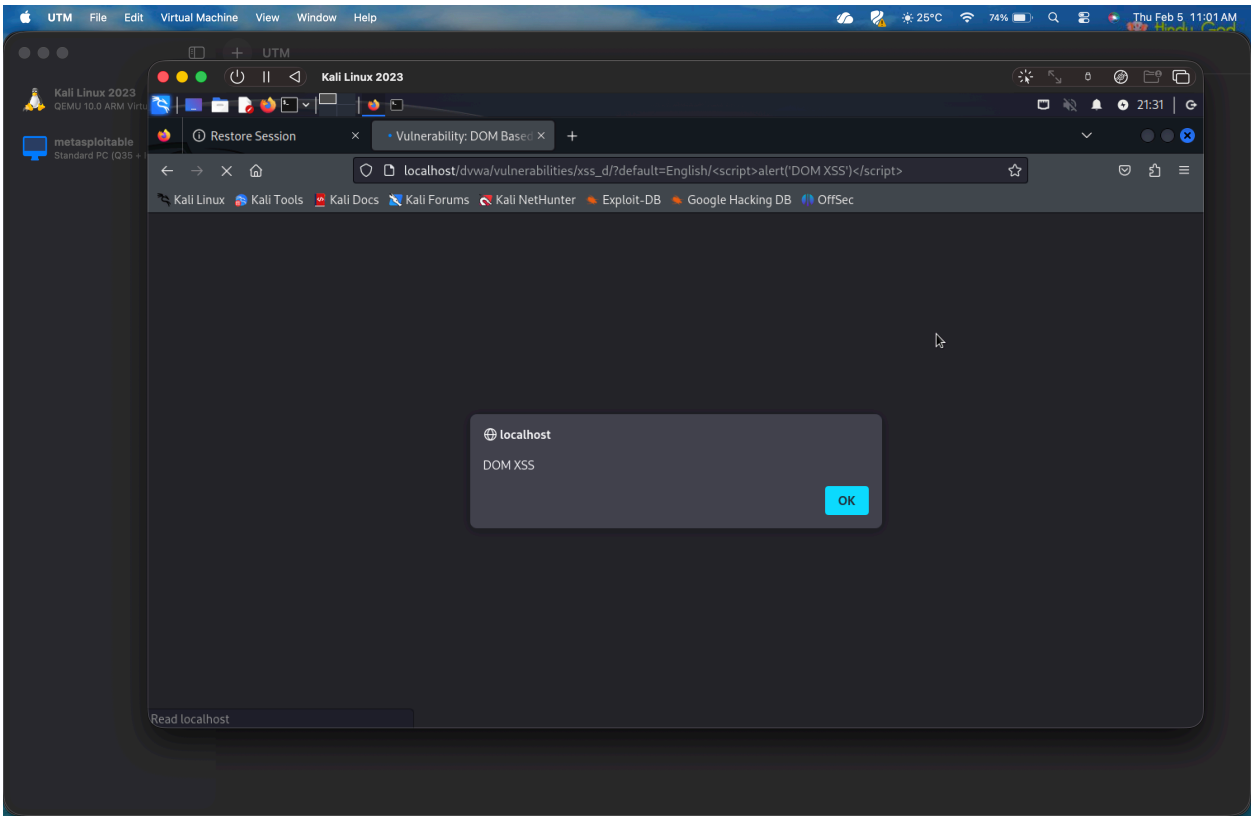
Refresh page → popup appears every time → Stored XSS successful.



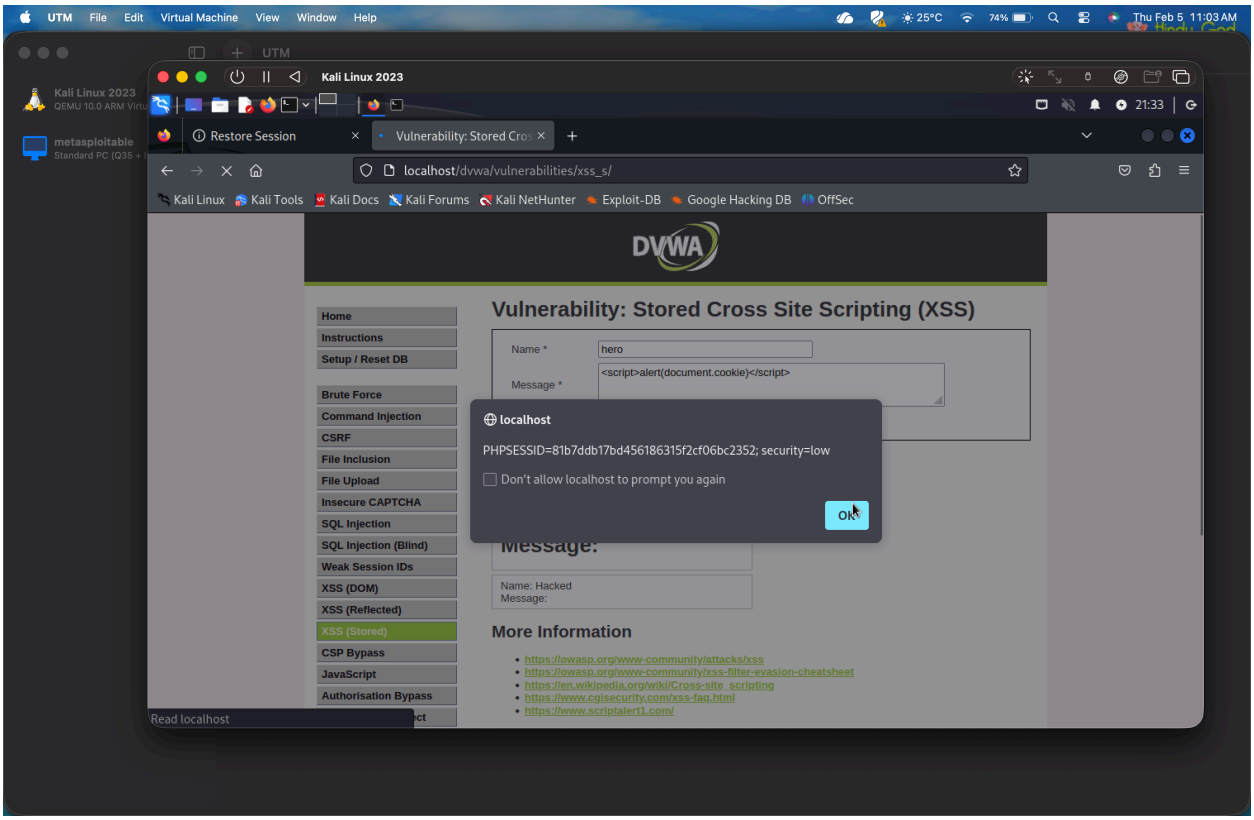
Step 5: DOM Based XSS
Go to:
DVWA → XSS (DOM)



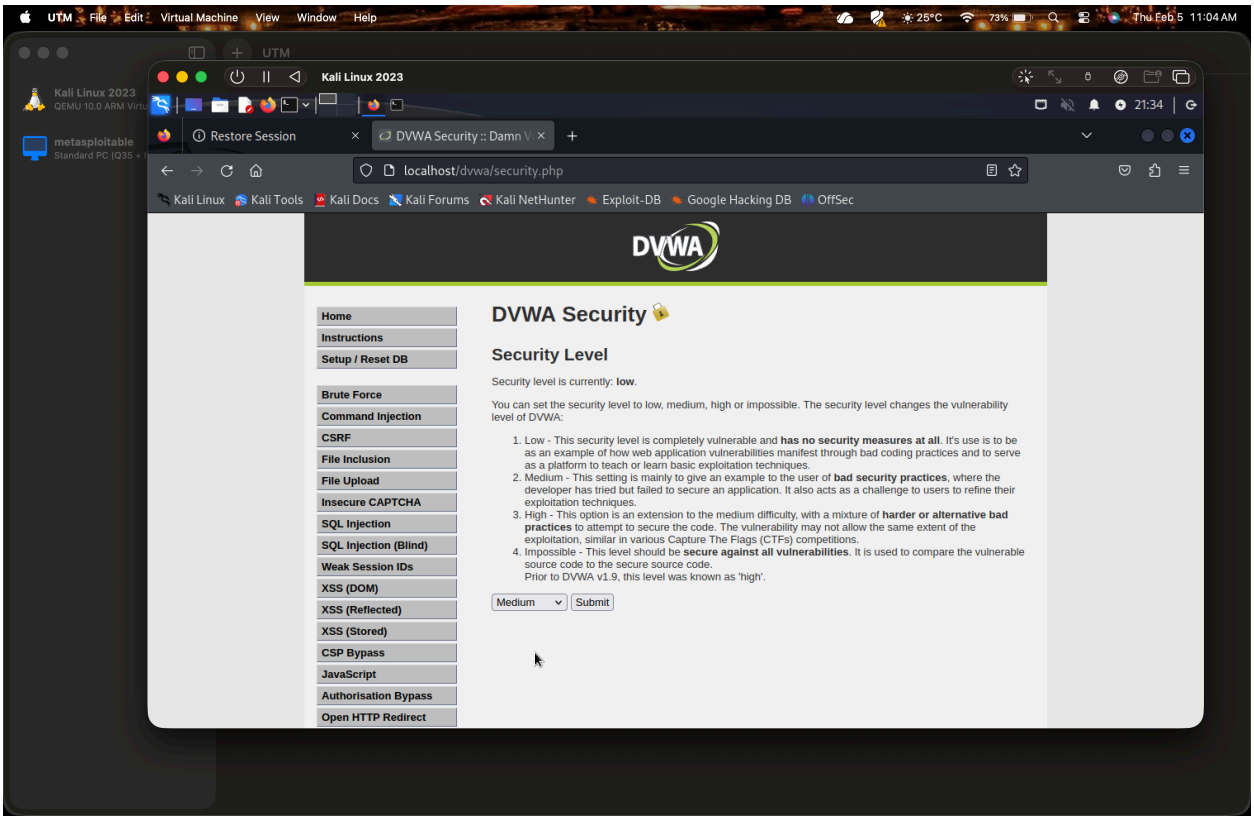
In the URL bar add:
#<script>alert('DOM XSS')</script>
Press Enter → popup appears.

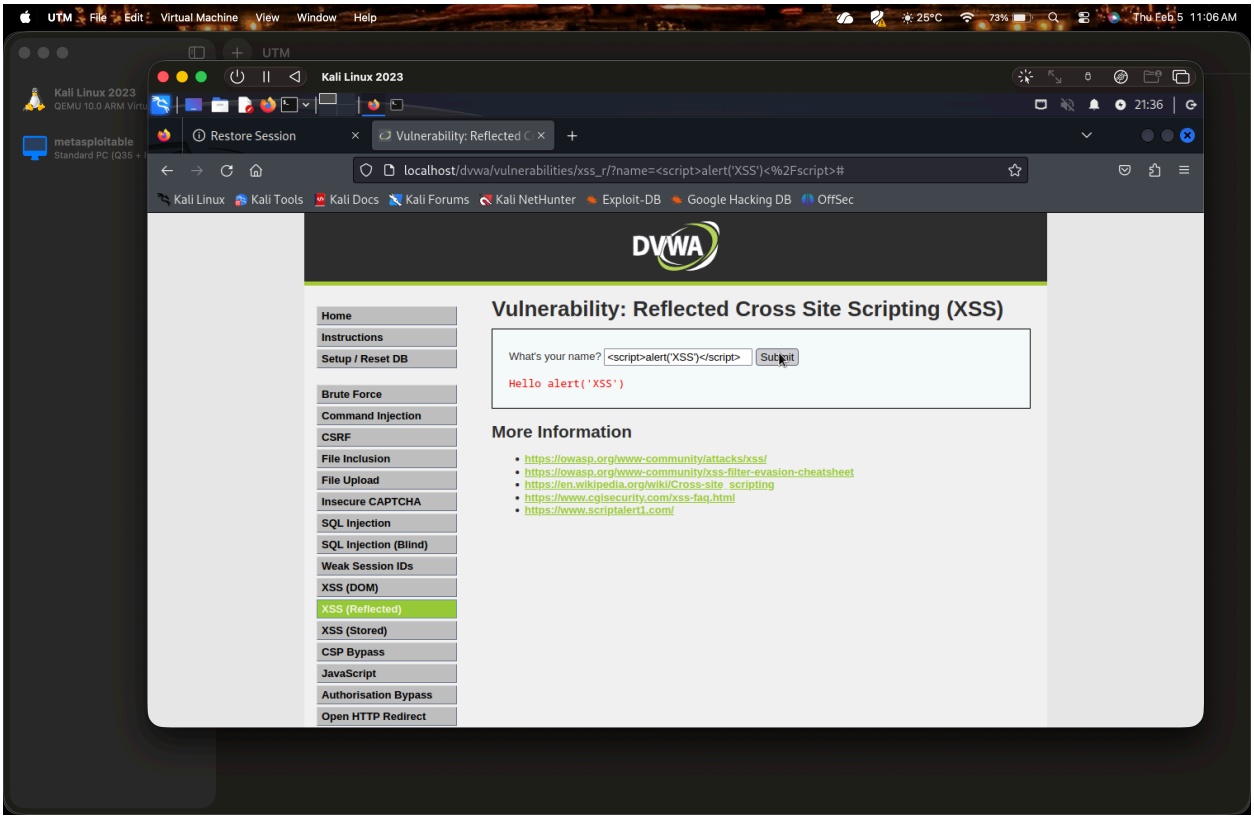


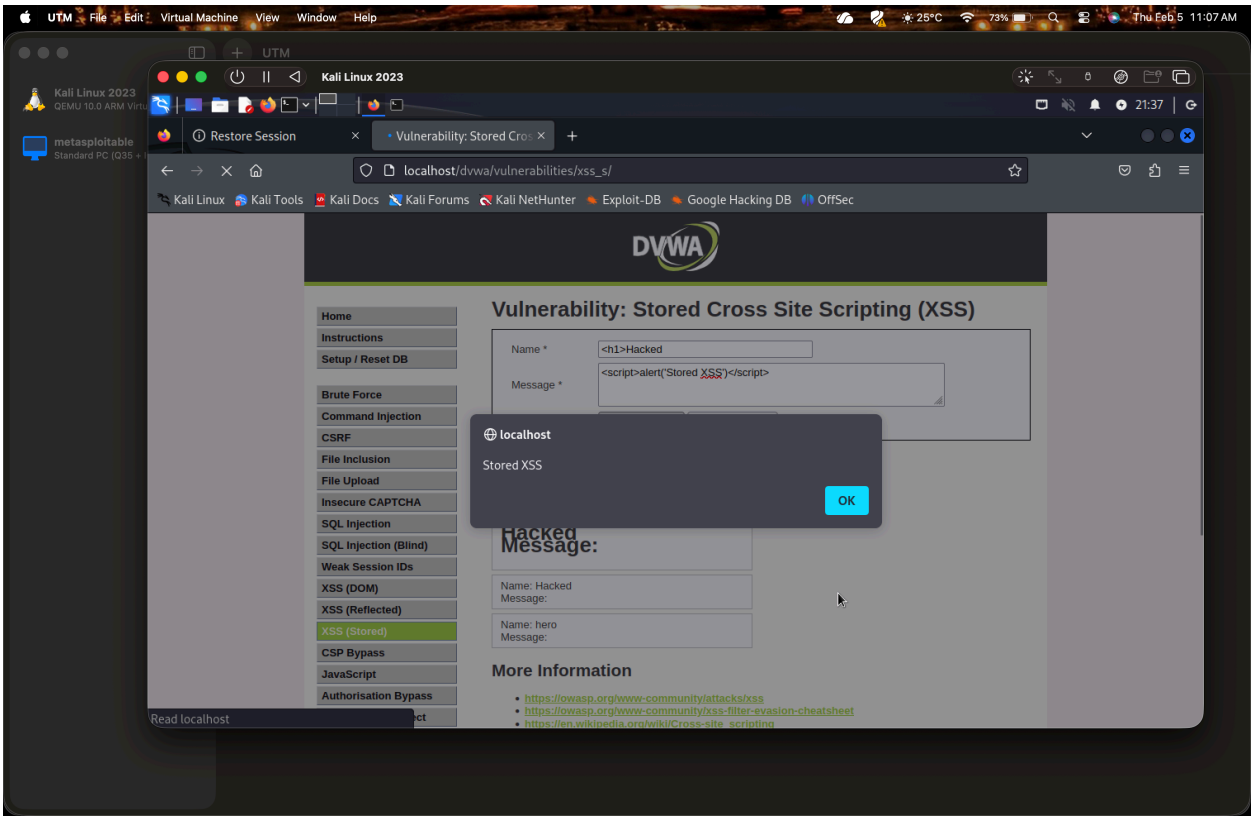
Step 6: Capture Cookie (Lab Demo)
In Stored XSS Message box:
<script>alert(document.cookie)</script>
This shows session cookies (demo of session theft).

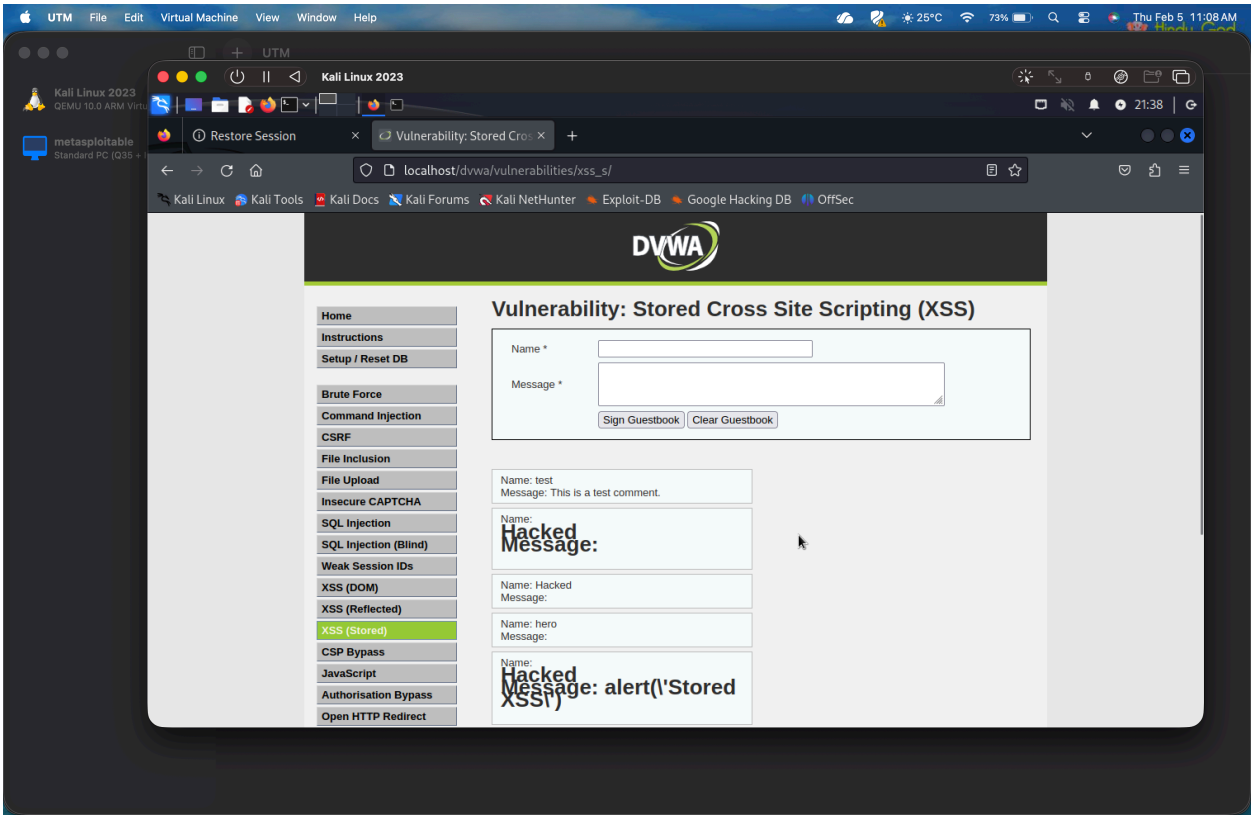


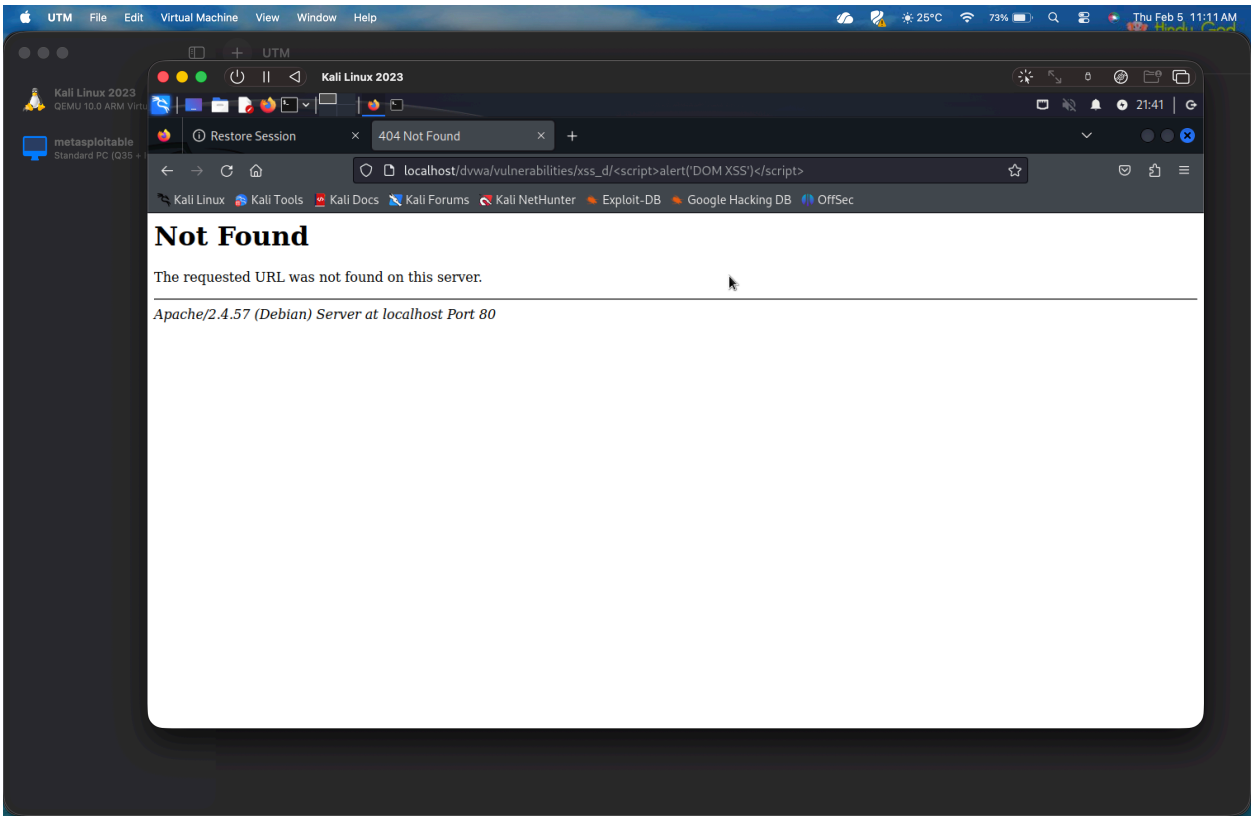
Step 7: Change Security Level
Go to DVWA Security → set:
• Medium
• High
Repeat the same payloads → see how filtering blocks them.

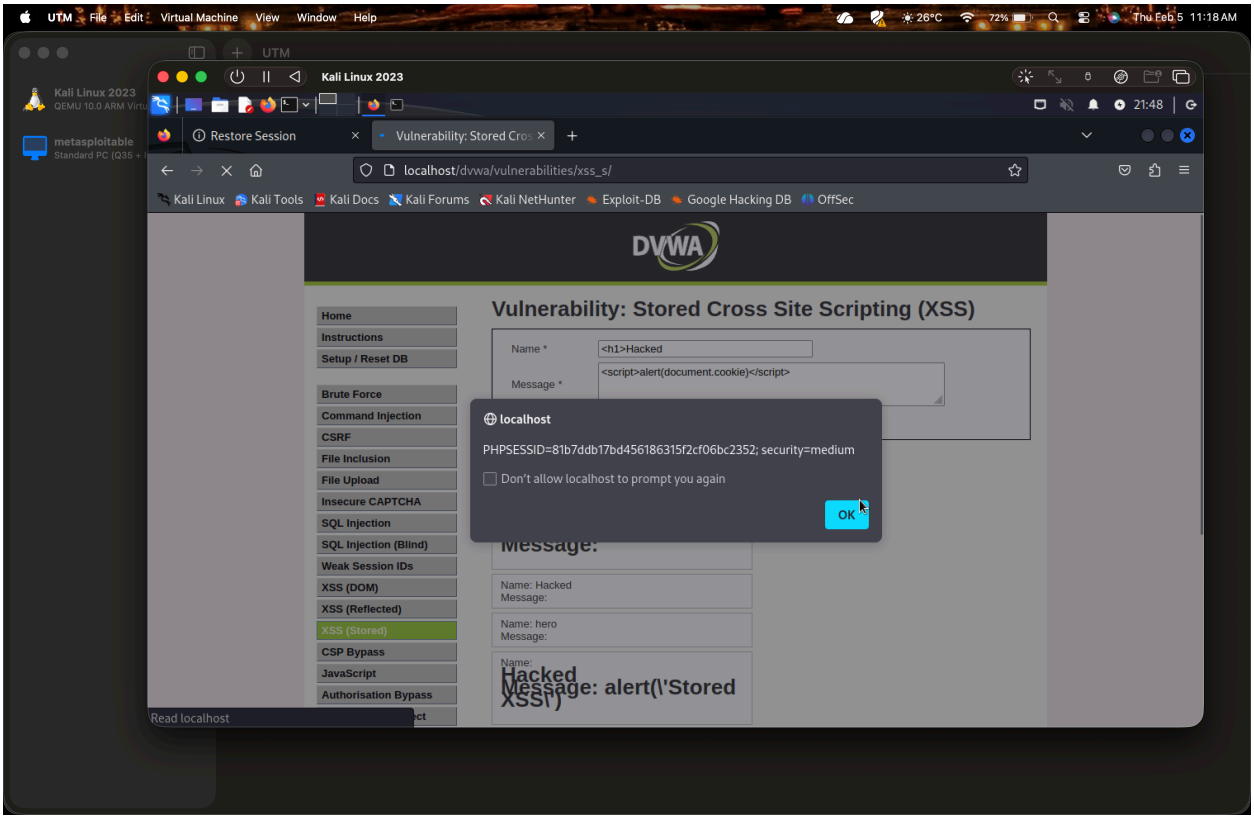

UTM File Edit Virtual Machine View Window Help
Thu Feb 5 11:04 AM
Kali Linux 2023
Restore Session
DVWA Security :: Damn V
localhost/dvwa/security.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command 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
DVWA Security
Security Level
Security level is currently: low.
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:
1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.
Medium
Submit

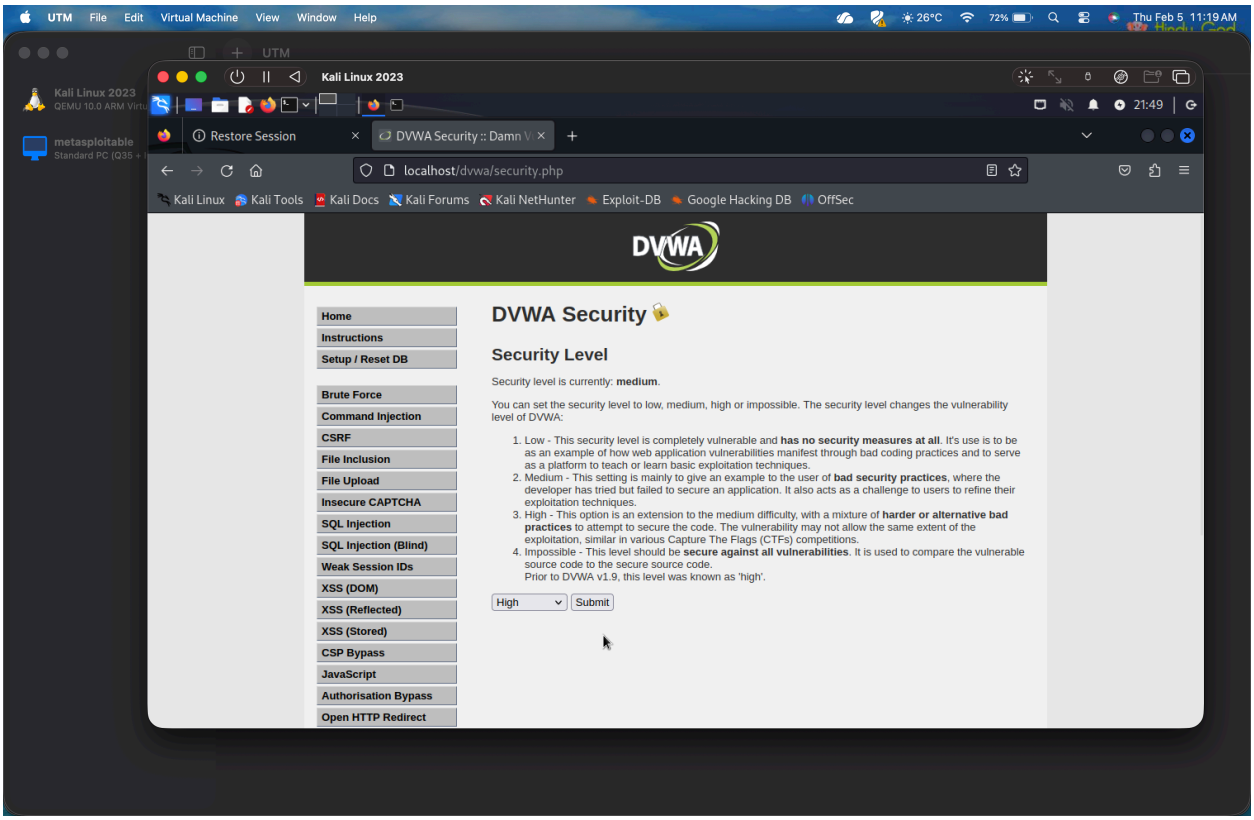

UTM File Edit Virtual Machine View Window Help
Thu Feb 5 11:06 AM
Kali Linux 2023
Restore Session
Vulnerability: Reflected C
localhost/dvwa/vulnerabilities/xss_r/?name=<script>alert('XSS')<%2Fscript>#
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
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
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name? <script>alert('XSS')</script>
Submit
Hello alert('XSS')
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
https://www.cgisecurity.com/xss-faq.html
https://www.scriptalert1.com/

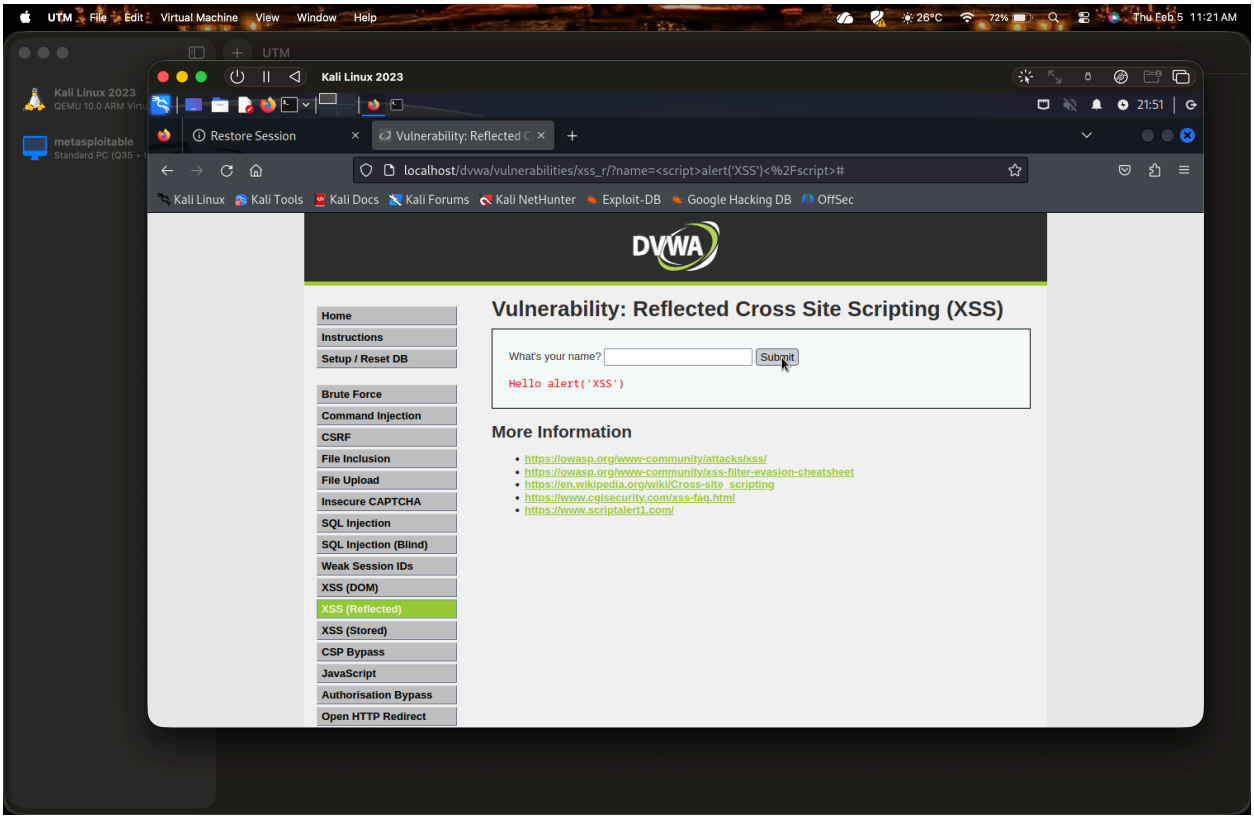

Kali Linux 2023
Restore Session
Vulnerability: Stored Cros
localhost/dvwa/vulnerabilities/xss_s/
DVWA
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
<h1>Hacked
Message *
<script>alert('Stored XSS')</script>
localhost
Stored XSS
OK
Hacked
Message:
Name: Hacked
Message:
Name: hero
Message:
More 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
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

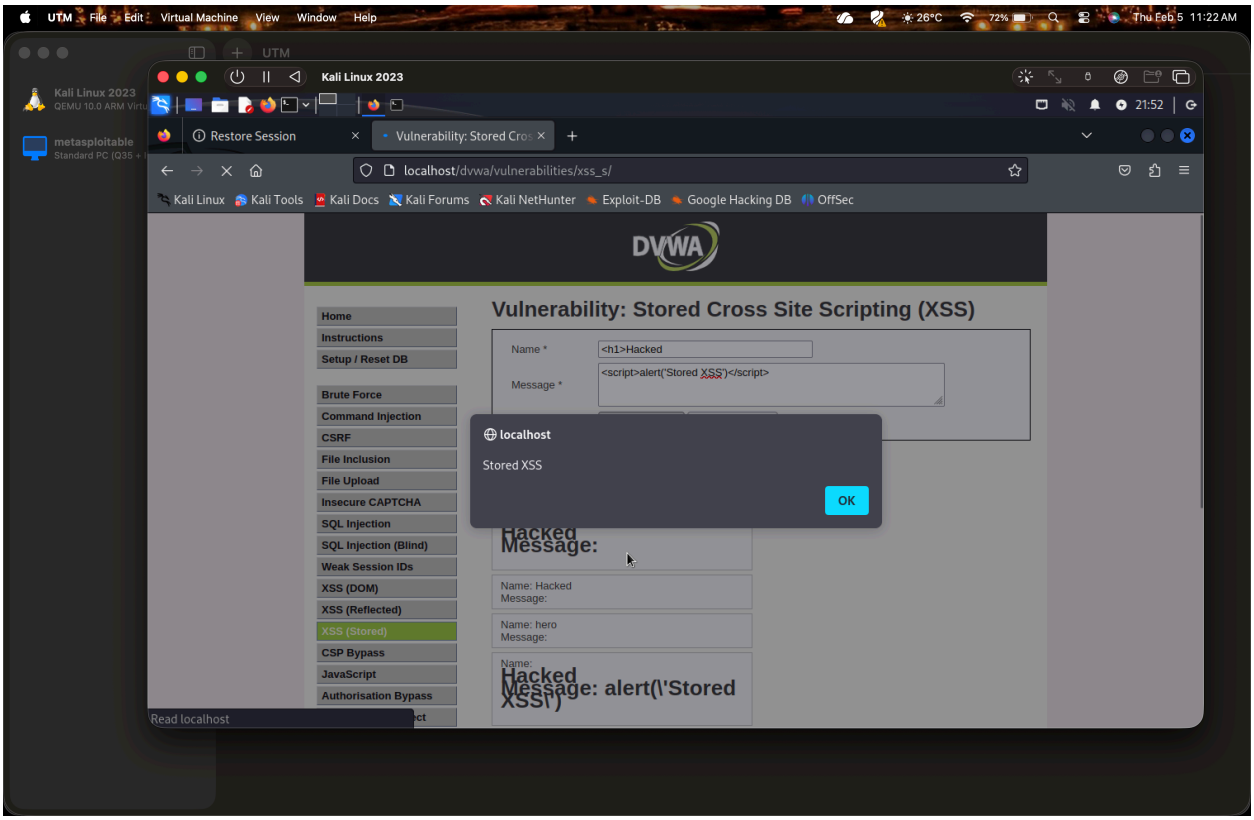

Kali Linux 2023
Restore Session
Vulnerability: Stored Cros
localhost/dvwa/vulnerabilities/xss_s/
DVWA
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
Sign Guestbook
Clear Guestbook
Name: test
Message: This is a test comment.
Name:
Hacked
Message:
Name: Hacked
Message:
Name: hero
Message:
Name:
Hacked
Message: alert(\'Stored XSS\')
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

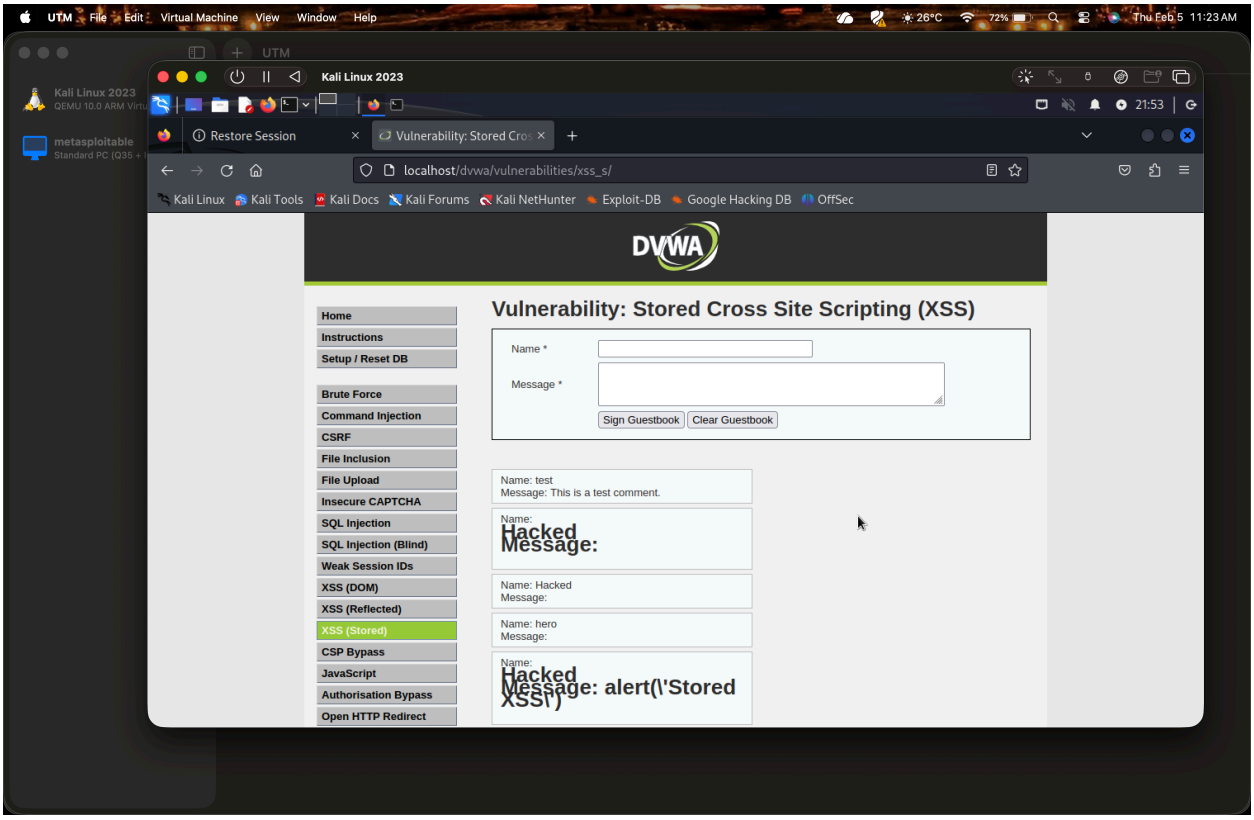

Kali Linux 2023
404 Not Found
localhost/dvwa/vulnerabilities/xss_d/<script>alert('DOM XSS')</script>
Not Found
The requested URL was not found on this server.
Apache/2.4.57 (Debian) Server at localhost Port 80

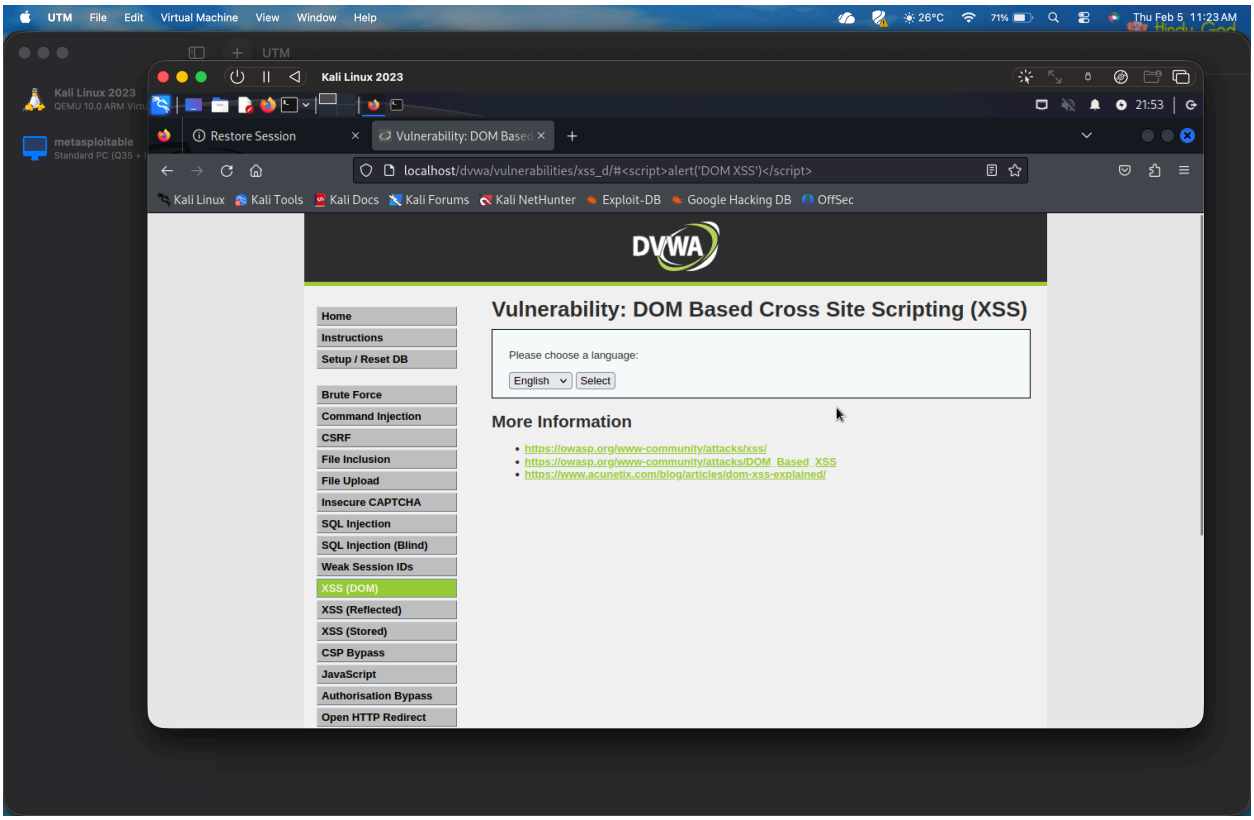

Kali Linux 2023
Vulnerability: Stored Cross Site Scripting (XSS)
localhost/dvwa/vulnerabilities/xss_s/
Name *
<h1>Hacked
Message *
<script>alert(document.cookie)</script>
localhost
PHPSESSID=81b7ddb17bd456186315f2cf06bc2352; security=medium
Don't allow localhost to prompt you again
OK
Name: Hacked
Message:
Name: hero
Message:
Hacked
Message: alert(\'Stored XSS\')

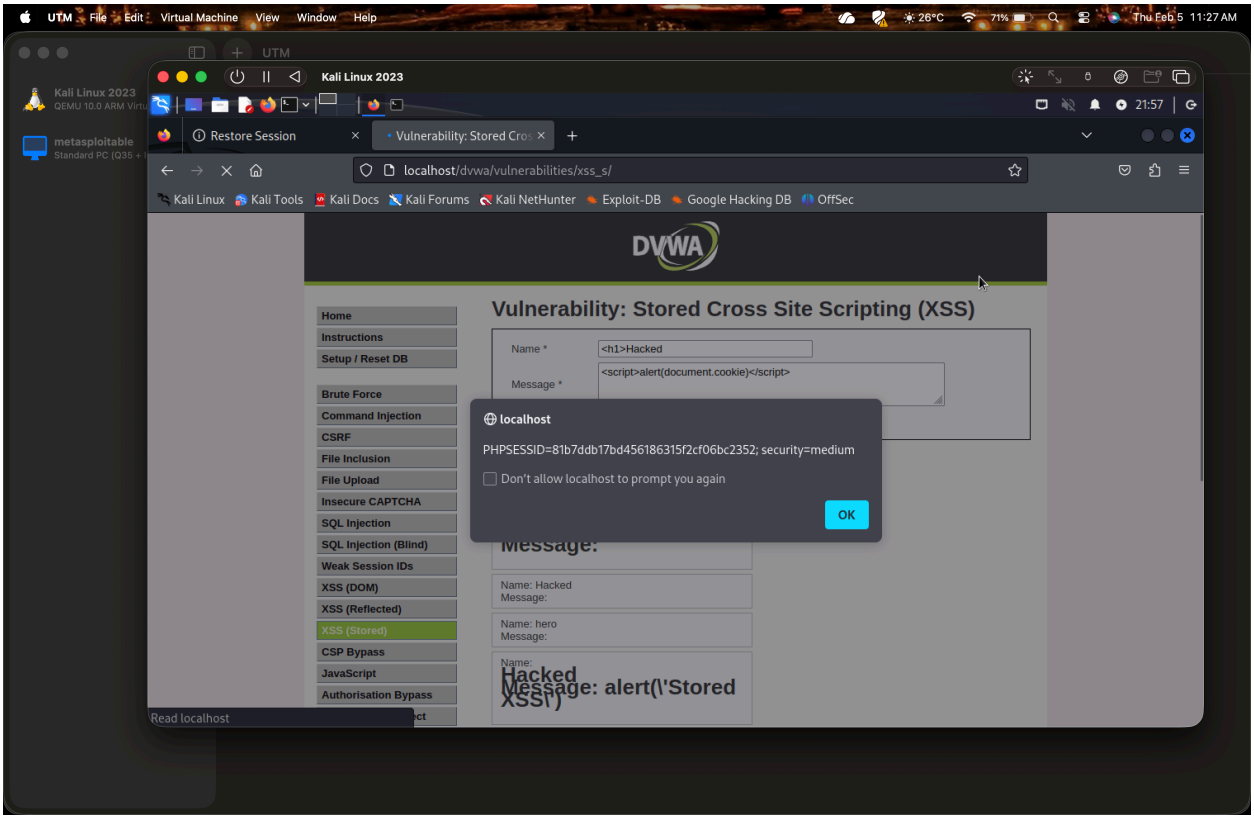

UTM File Edit Virtual Machine View Window Help
Thu Feb 5 11:19 AM
Kali Linux 2023
Restore Session
DVWA Security :: Damn V
localhost/dvwa/security.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
DVWA
Home
Instructions
Setup / Reset DB
Brute Force
Command 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
DVWA Security
Security Level
Security level is currently: medium.
You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:
1. Low - This security level is completely vulnerable and has no security measures at all. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of bad security practices, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of harder or alternative bad practices to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be secure against all vulnerabilities. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.
High
Submit


UTM File Edit Virtual Machine View Window Help
Thu Feb 5 11:21 AM
Kali Linux 2023
Restore Session
Vulnerability: Reflected C
localhost/dvwa/vulnerabilities/xss_r/?name=<script>alert('XSS')<%2Fscript>#
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello alert('XSS')
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
https://www.cgisecurity.com/xss-faq.html
https://www.scriptalert1.com/


Kali Linux 2023
Restore Session
Vulnerability: Stored Cros
localhost/dvwa/vulnerabilities/xss_s/
DVWA
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
<h1>Hacked
Message *
<script>alert('Stored XSS')</script>
localhost
Stored XSS
OK
Name: Hacked
Message:
Name: hero
Message:
Hacked
Message: alert(\'Stored
XSS\')
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


Kali Linux 2023
Restore Session
Vulnerability: Stored Cros
localhost/dvwa/vulnerabilities/xss_s/
DVWA
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
Message *
Sign Guestbook
Clear Guestbook
Name: test
Message: This is a test comment.
Name:
Hacked
Message:
Name: Hacked
Message:
Name: hero
Message:
Hacked
Message: alert(\'Stored
XSS\')
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


Kali Linux 2023
Restore Session
Vulnerability: DOM Based
localhost/dvwa/vulnerabilities/xss_d/#<script>alert('DOM XSS')</script>
DVWA
Vulnerability: DOM Based Cross Site Scripting (XSS)
Please choose a language:
English
Select
More Information
https://owasp.org/www-community/attacks/xss/
https://owasp.org/www-community/attacks/DOM_Based_XSS
https://www.acunetix.com/blog/articles/dom-xss-explained/
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


Kali Linux 2023
Restore Session
Vulnerability: Stored Cros
localhost/dvwa/vulnerabilities/xss_s/
DVWA
Vulnerability: Stored Cross Site Scripting (XSS)
Name *
<h1>Hacked
Message *
<script>alert(document.cookie)</script>
localhost
PHPSESSID=81b7ddb17bd456186315f2cf06bc2352; security=medium
Don't allow localhost to prompt you again
OK
Name: Hacked
Message:
Name: hero
Message:
Hacked
Message: alert(\'Stored XSS\')
Read localhost
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