LAB #6: SQL Injection

Destiny Hale

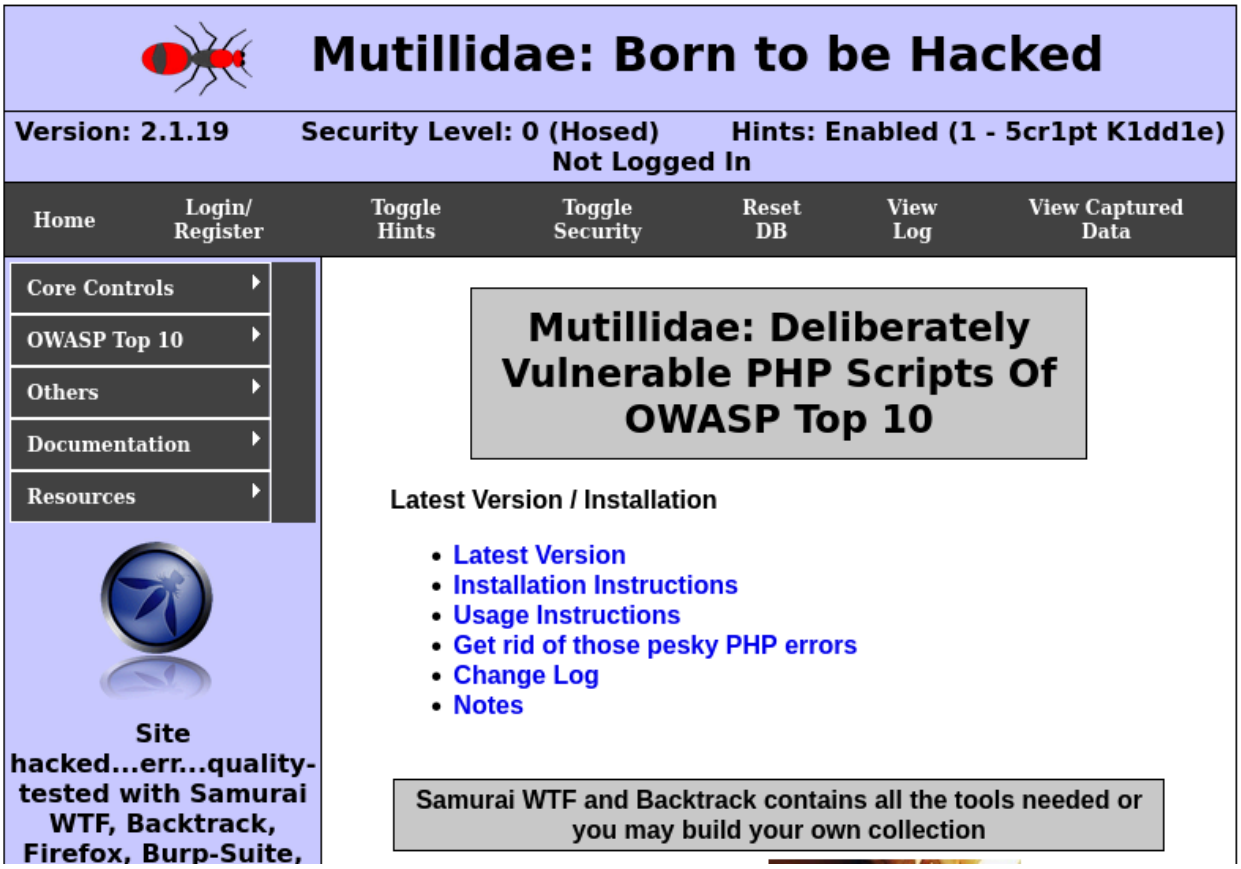
11/20/25

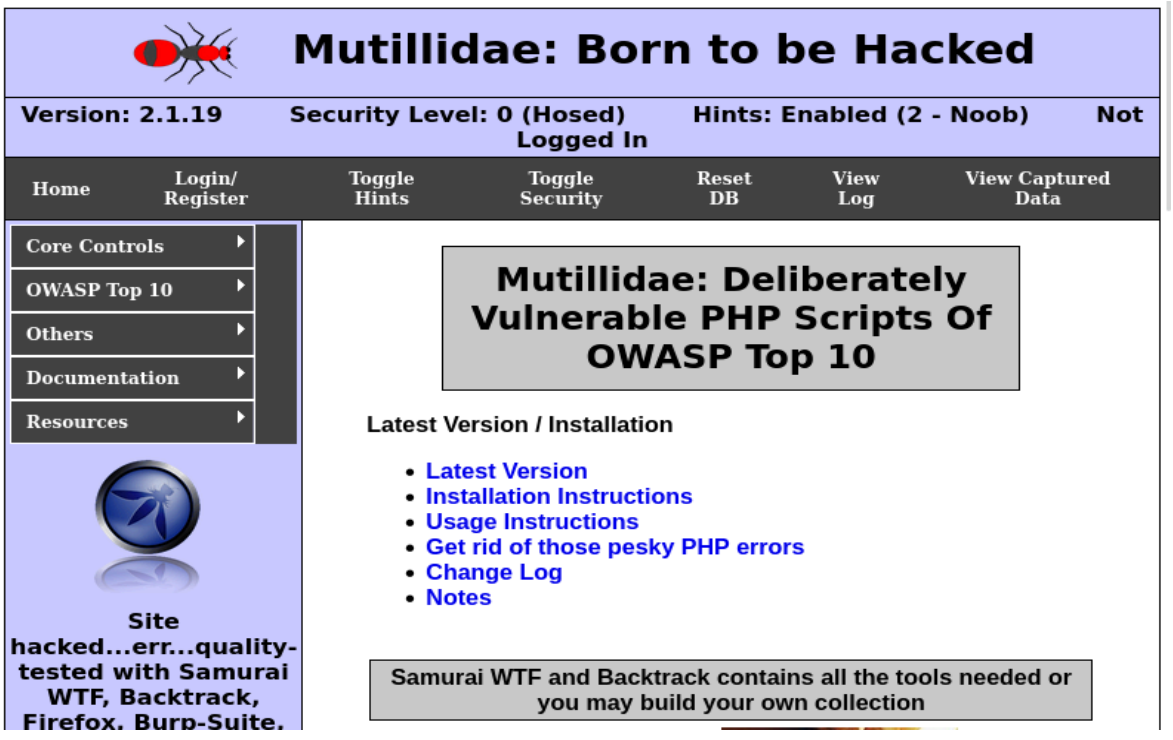
6) Select SQL Injection from the menu and enter any value other than 2 as the User ID. Submit the user id and take a screenshot like the attached one showing the result. Briefly explain how SQL Injection can be implemented to get the same result. Give the relevant SQL query you need to use. 10 points

- To get the same result, without using the bar, the attacker would use an SQL query such as 3'OR '1'='1 to gain the first name and surname of user 3.

7) In Firefox, go the following URL: http://<Metasploitable 2 IP>/multillidae/ You will get a page like this. Click multiple times on the buttons "Toggle Security" and "Toggle Hints". Briefly explain what happens when you change these settings. Take relevant screenshots to attach to your submission. 4 Points

Clicking toggle hints:

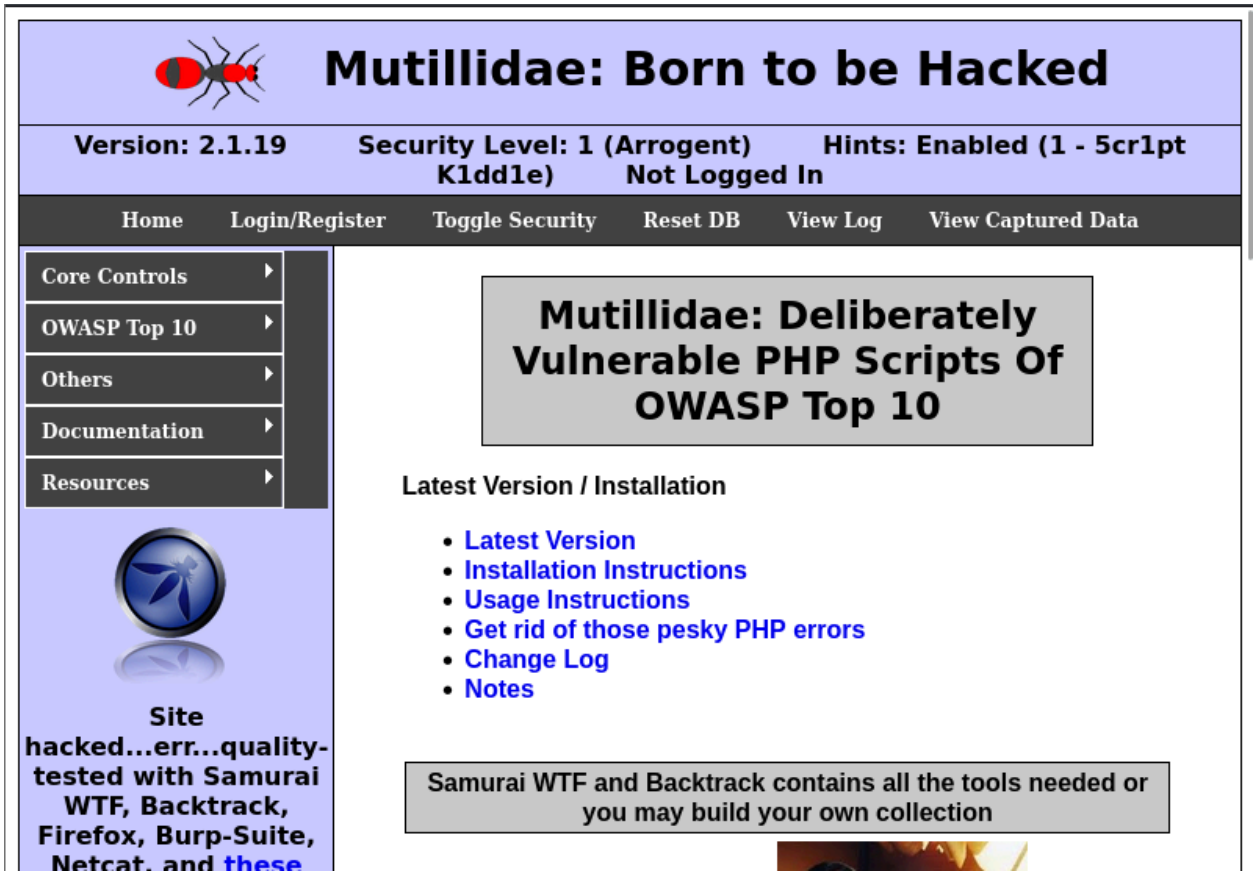




Clicking toggle security:

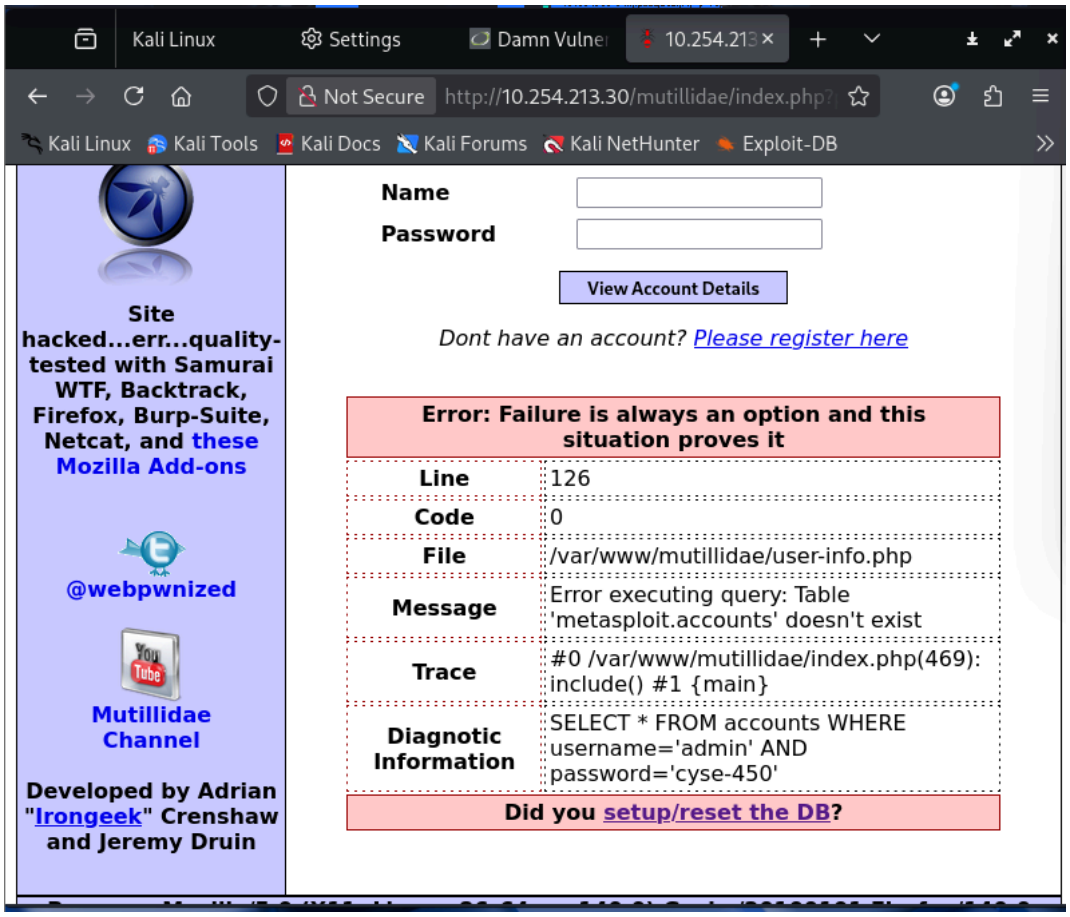

Kali Linux
Settings
Damn Vulne
10.254.213
Not Secure
http://10.254.213.30/mutillidae/index.php?
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Mutillidae: Born to be Hacked
Version: 2.1.19
Security Level: 1 (Arrogent)
Hints: Disabled (0 - I try harder)
Not Logged In
Home
Login/Register
Toggle Security
Reset DB
View Log
View Captured Data
Core Controls
OWASP Top 10
Others
Documentation
Resources
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these
Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10
Latest Version / Installation
Latest Version
Installation Instructions
Usage Instructions
Get rid of those pesky PHP errors
Change Log
Notes
Samurai WTF and Backtrack contains all the tools needed or you may build your own collection


Not Secure
http://10.254.213.30/mutillidae/index.php?
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Mutillidae: Born to be Hacked
Version: 2.1.19
Security Level: 5 (Secure)
Hints: Disabled (0 - I try harder)
Not Logged In
Home
Login/Register
Toggle Security
Reset DB
View Log
View Captured Data
Core Controls
OWASP Top 10
Others
Documentation
Resources
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these
Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10
Latest Version / Installation
Latest Version
Installation Instructions
Usage Instructions
Get rid of those pesky PHP errors
Change Log
Notes
Samurai WTF and Backtrack contains all the tools needed or you may build your own collection


Mutillidae: Born to be Hacked
Version: 2.1.19
Security Level: 1 (Arrogent)
Hints: Enabled (1 - 5cr1pt K1dd1e)
Not Logged In
Home
Login/Register
Toggle Security
Reset DB
View Log
View Captured Data
Core Controls
OWASP Top 10
Others
Documentation
Resources
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these
Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10
Latest Version / Installation
Latest Version
Installation Instructions
Usage Instructions
Get rid of those pesky PHP errors
Change Log
Notes
Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

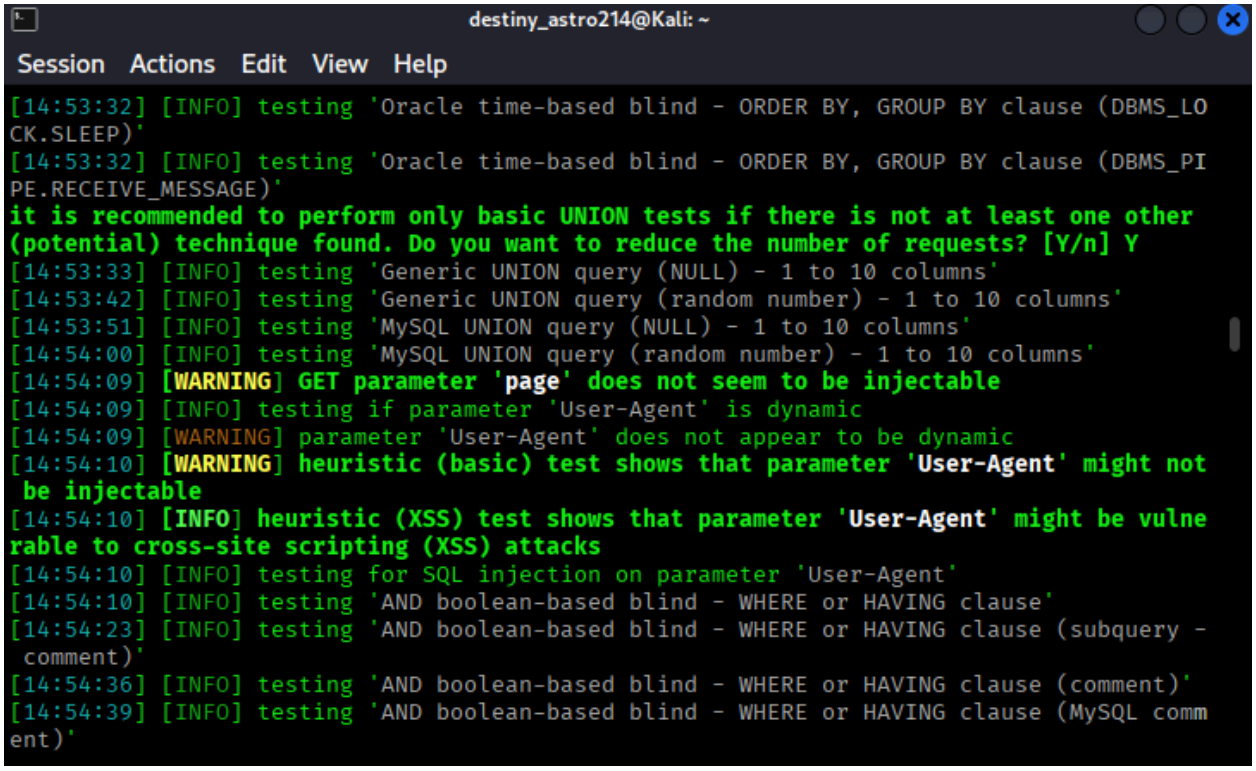
- While clicking both settings multiple times, the security levels change to either 0, 1, or 5. As for the hints, they switch from script-kiddie to noob. The toggle hint setting also disappears as I click the toggle security setting multiple times.

9) Similar to the following screenshot, show the SQL query that has been executed. Note that you used the password "cyse-450", not "password". If you get an error message like the message shown in the screenshot, explain the reason behind this error. If there is no error message, take screenshots of the resultant output. 6 points



- The reasoning behind this error message is that the login I used doesn't exist within metasploit's table.

10) Run the sqlmap command shown in the following screenshot in your Kali Terminal. Take necessary screenshots showing your results. 4 points



11) Explore different features of the Multillidae application and provide a brief comparison with the DVWA application. Make sure you discuss the features of both applications in your comparative discussion. 6 points

- Both Mutillidae and DVWA are vulnerable web applications that provides numerous vulnerabilities for you to test. With Mutillidae, this tool provides the top ten vulnerabilities that were recorded in OWASP. This also provides numerous injection vulnerabilities such as cookie injection, SQL injection, HTML injection and more. As for testing, this gives you hints and tutorials on how to execute these attacks. On the other hand, DVWA provides simple attacks such as SQL injection, XSS, brute force, and command execution. This website focuses on common vulnerabilities and provides documentation. As for testing, you can insert any query to see how each vulnerability works.