

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:



Mutillidae: Born to be Hacked

Version: 2.1.19

Security Level: 0 (Hosed)
Not Logged In

Hints: Enabled (1 - 5cr1pt K1dd1e)

Home

Login/
Register

Toggle
Hints

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,

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: 0 (Hosed)
Logged In

Hints: Enabled (2 - Noob)

Not

Home

Login/
Register

Toggle
Hints

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.

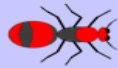
Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

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

Clicking toggle security:



Mutillidae: Born to be Hacked

Version: 2.1.19

Security Level: 1 (Arrogant)

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: 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 (Arrogant Kiddle)** **Hints: Enabled (1 - 5cr1pt)**
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

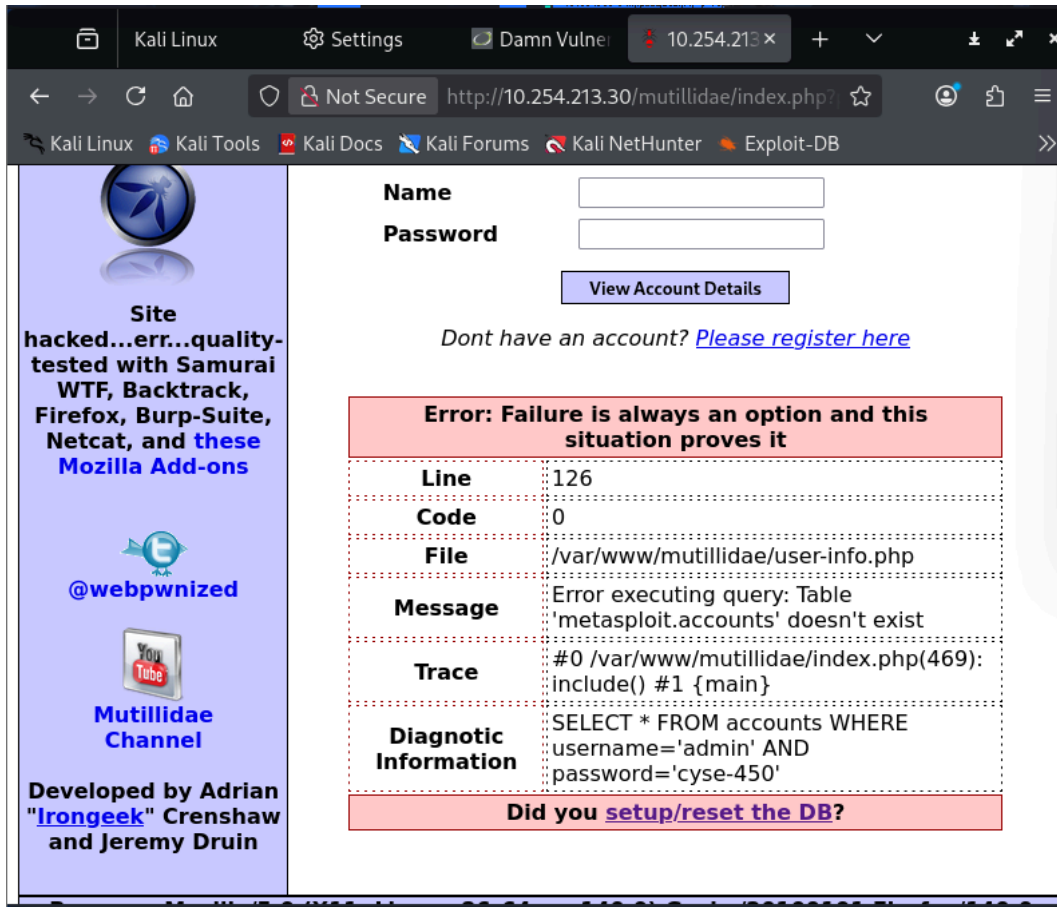
Latest Version / Installation

- [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

```
destiny_astro214@Kali: ~
Session Actions Edit View Help
[14:53:32] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LO
CK.SLEEP)
[14:53:32] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PI
PE.RECEIVE_MESSAGE)
it is recommended to perform only basic UNION tests if there is not at least one other
(potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[14:53:33] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[14:53:42] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
[14:53:51] [INFO] testing 'MySQL UNION query (NULL) - 1 to 10 columns'
[14:54:00] [INFO] testing 'MySQL UNION query (random number) - 1 to 10 columns'
[14:54:09] [WARNING] GET parameter 'page' does not seem to be injectable
[14:54:09] [INFO] testing if parameter 'User-Agent' is dynamic
[14:54:09] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[14:54:10] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not
be injectable
[14:54:10] [INFO] heuristic (XSS) test shows that parameter 'User-Agent' might be vulne
rable to cross-site scripting (XSS) attacks
[14:54:10] [INFO] testing for SQL injection on parameter 'User-Agent'
[14:54:10] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[14:54:23] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery -
comment)'
[14:54:36] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[14:54:39] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comm
ent)'
```

11) Explore different features of the Mutillidae 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.