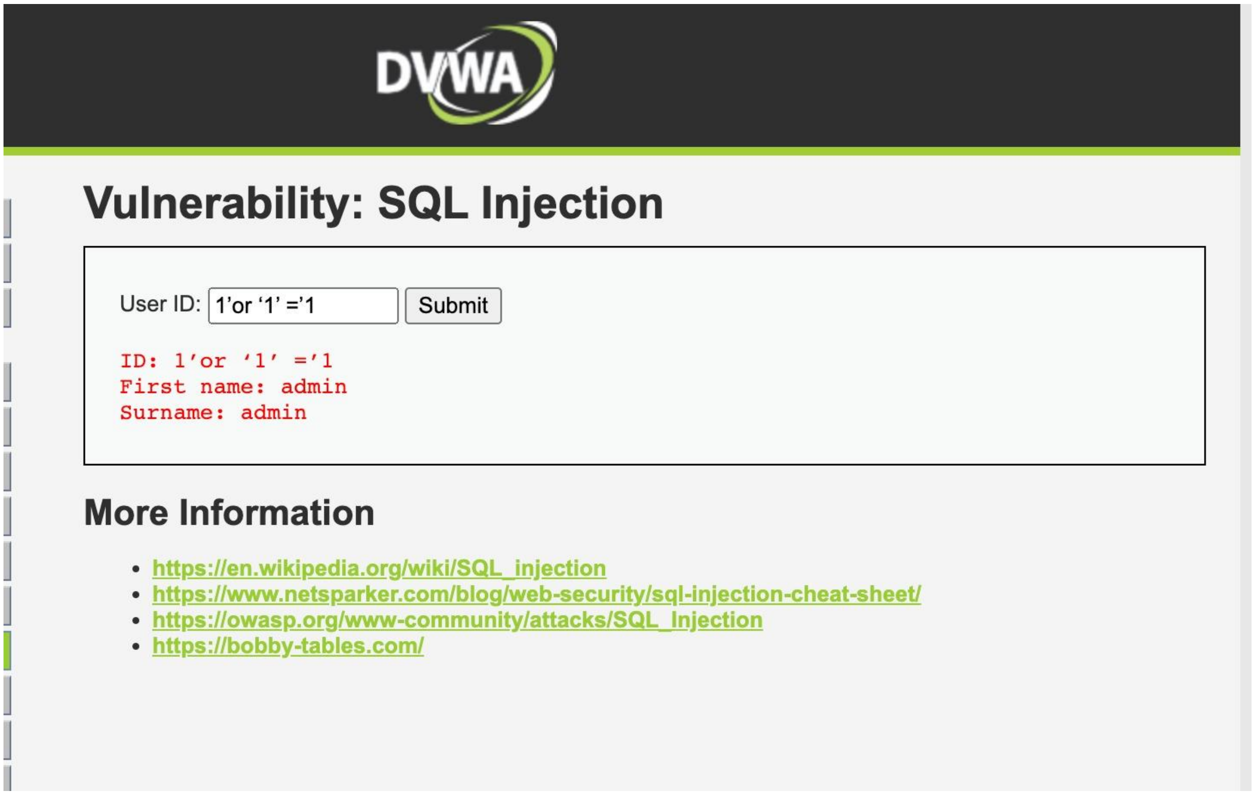
CMPE-279 Assignment-3

Ayush Gupta(Sjsu id: 014952184)
Chetan Nain(Sjsu id: 015761122)

**Q.1 Describe the SQLi attack you used, how did you cause the user table to be dumped? What was the input string you used?**

Ans: SQLi Injection is a way in which sensitive data can be hacked by modifying sql query. After setting the security level to low we ran the input string as 1’or ‘1’ =’1 . This string will get converted to sql query to:
“Select first_name, last_name From users where ‘1’ = ‘1;”;
This query will always return true for second condition which is after OR as 1 will be always equal to 1. And this way we were able to extract data from the database.



Vulnerability: SQL Injection

User ID: 1’or ‘1’ =’1

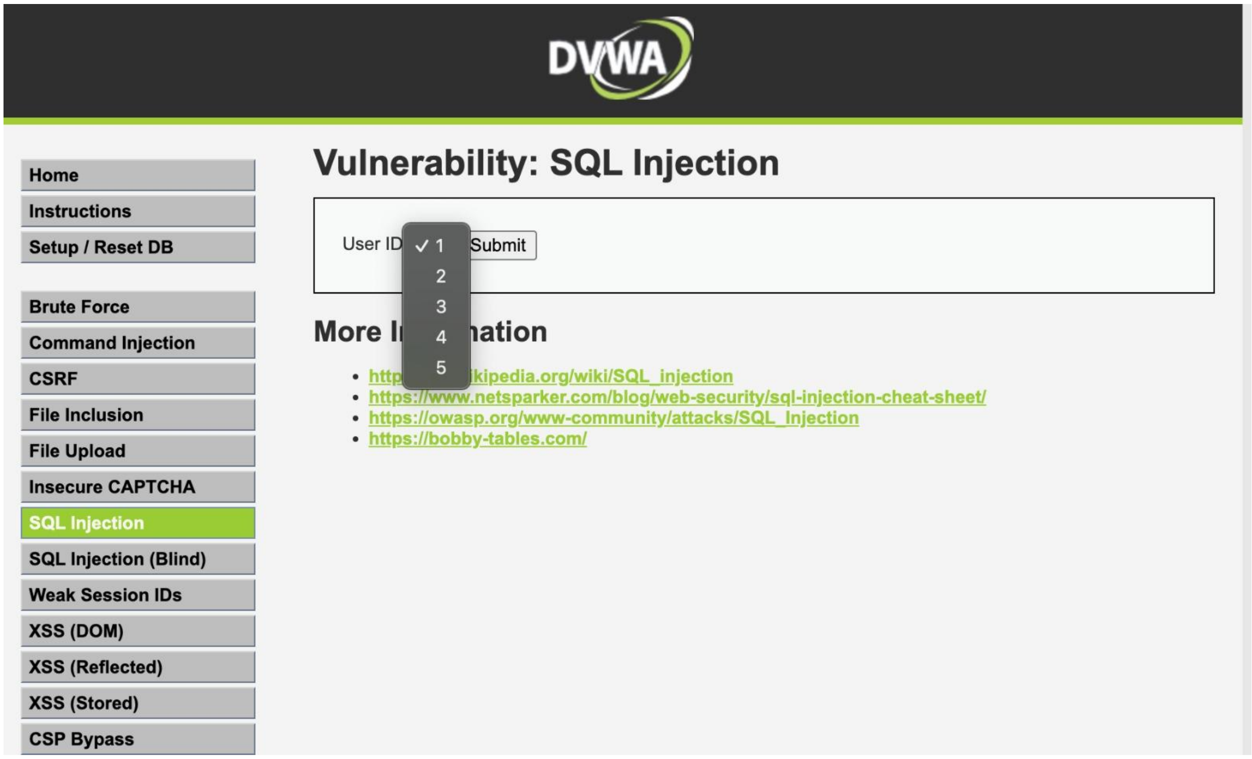
```
ID: 1’or ‘1’ =’1
First name: admin
Surname: admin
```

More Information

- https://en.wikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

**Q.2 If you switch the security level in DVWA to “Medium”, does the SQLi attack still work?**

Ans2: No, we were not able to perform the SQLi attack through same string as instead of textbox we had dropdown list and thus we had to select the id from the given list. So we can say vulnerability is handled in this case by using dropdown instead of textbox entry.



Vulnerability: SQL Injection

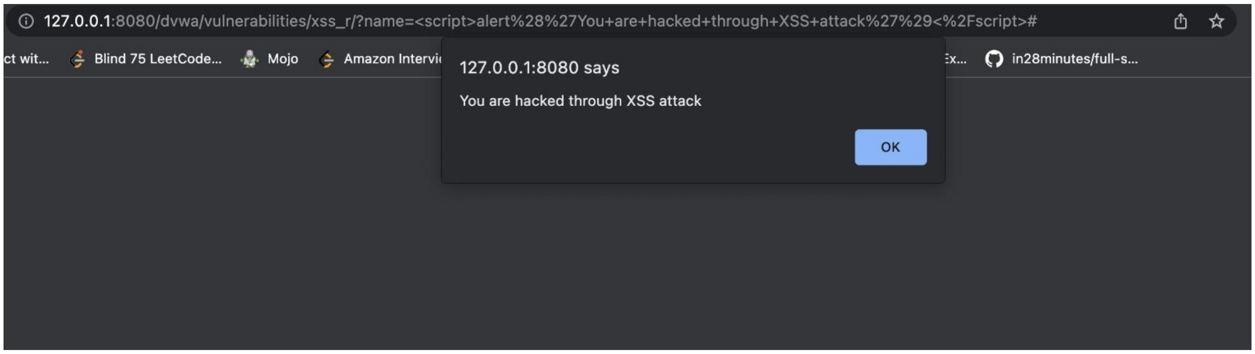
More I nation

- http ikipedia.org/wiki/SQL_injection
- https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
- https://owasp.org/www-community/attacks/SQL_Injection
- https://bobby-tables.com/

**Q.3 Describe the reflected XSS attack you used, how did it work?**

Ans3: Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. When we checked source for the application page, we found there was no restrictions on the input field. So we tried using

<script>alert(“You are hacked through XSS attack”)</script>. Using this way, we got a javascript popup alert.



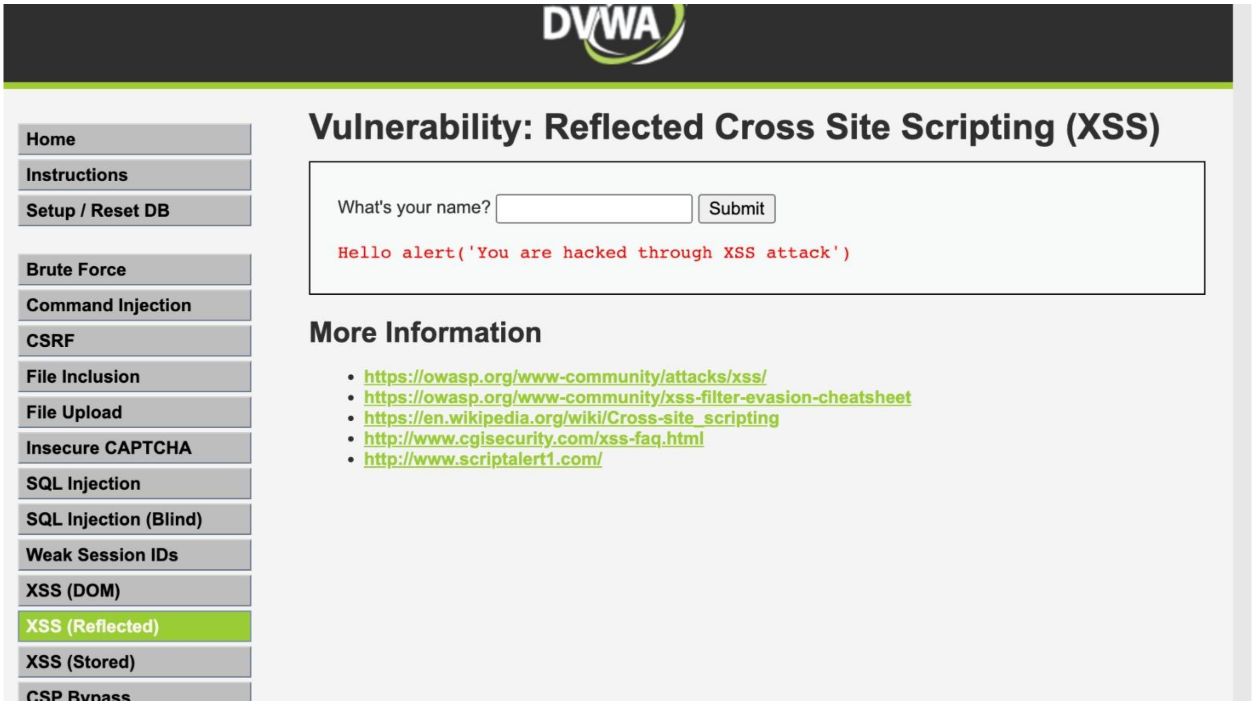
127.0.0.1:8080/dvwa/vulnerabilities/xss_r/?name=<script>alert%28%27You+are+hacked+through+XSS+attack%27%29<%2Fscript>#

127.0.0.1:8080 says

You are hacked through XSS attack

**Q.4 If you switch the security level in DVWA to "Medium", does the XSS attack still work?**

Ans4: No, since with Medium security, we saw restriction on the input field. the script tag was getting replaced with empty thus removing our script tag. Hence we were not able to exploit XSS vulnerability in the same way.



Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? Submit

```
Hello alert('You are hacked through XSS attack')
```

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
- http://www.cgisecurity.com/xss-faq.html
- http://www.scriptalert1.com/