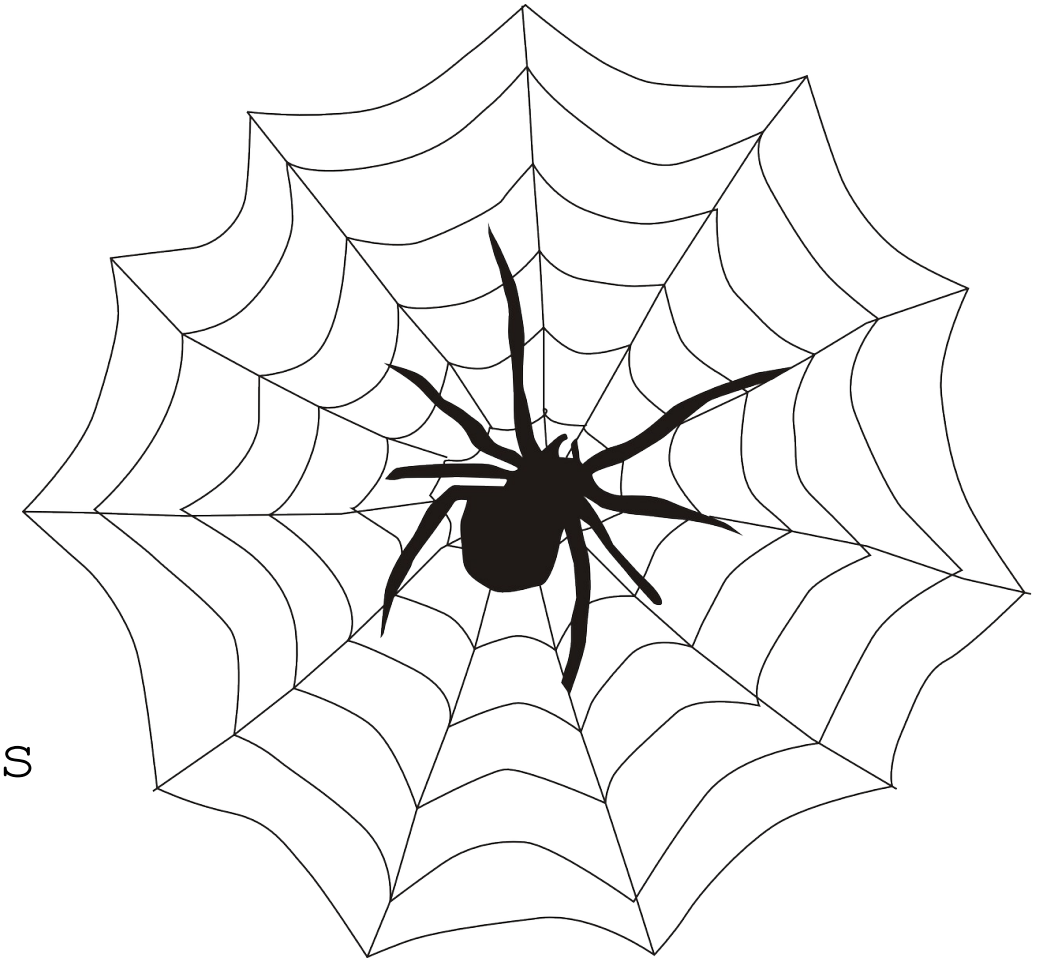
HackerFrogs Afterschool SQL Injection /w TryHackMe

Class:
Web App Hacking

Workshop Number:
AS-WEB-07

Document Version:
1.5

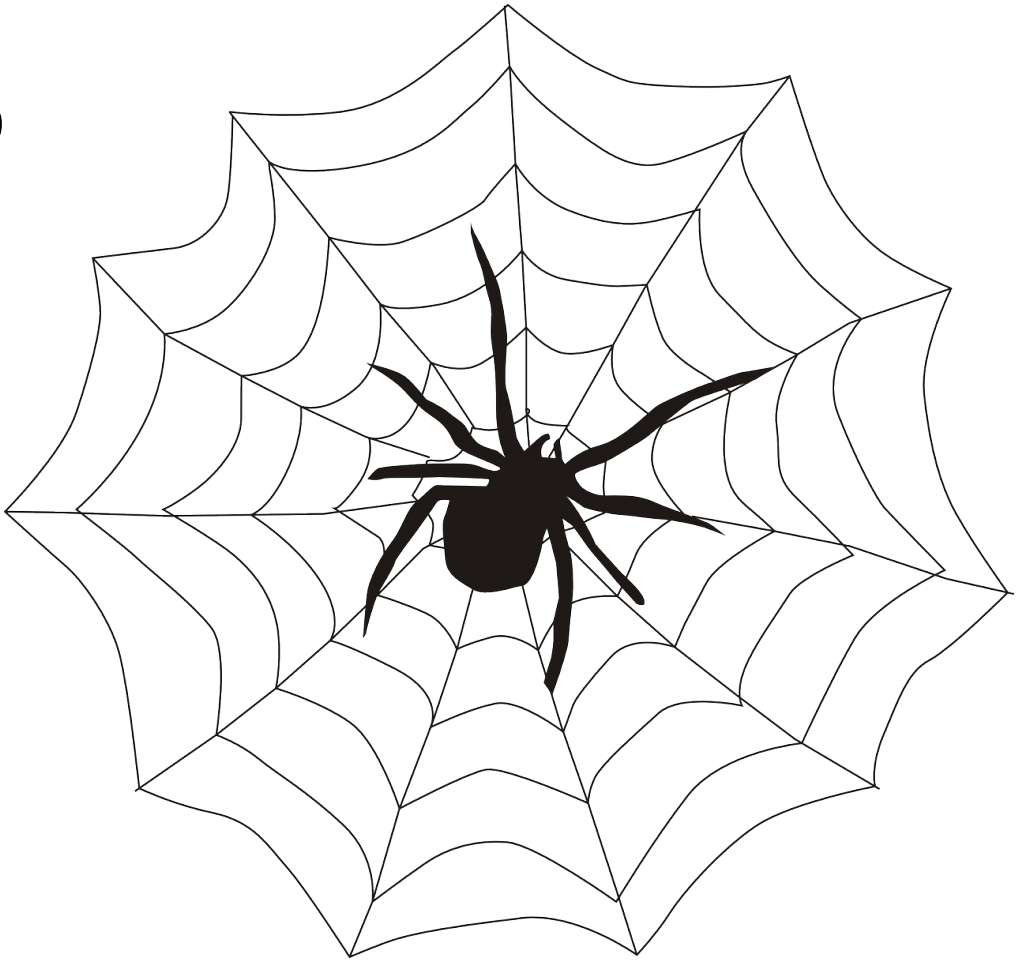
Special Requirements:
Completion of previous workshop, AS-WEB-06.
Registered account at tryhackme.com



What We Learned In The Previous Workshop

This is the seventh intro to web app hacking workshop.

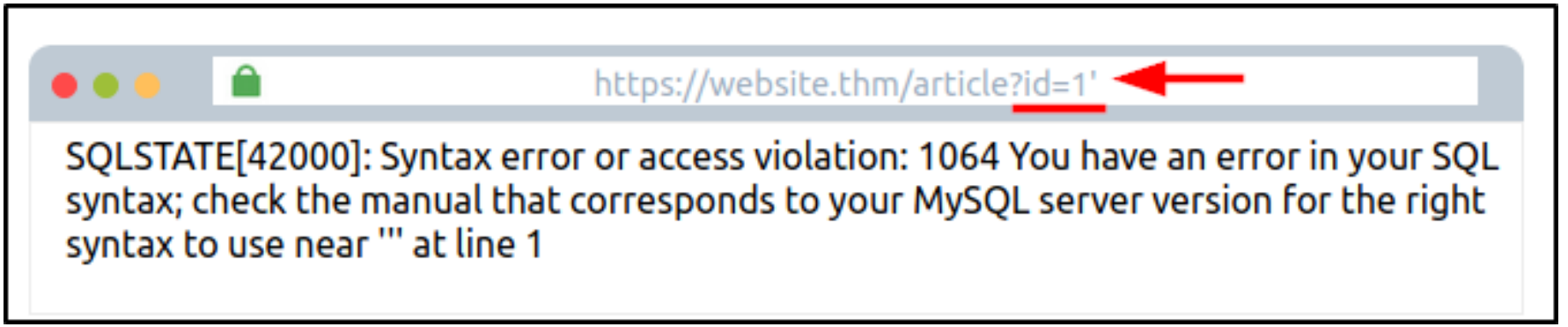
In the previous workshop we learned about the following web app hacking concepts:



SQL Injection

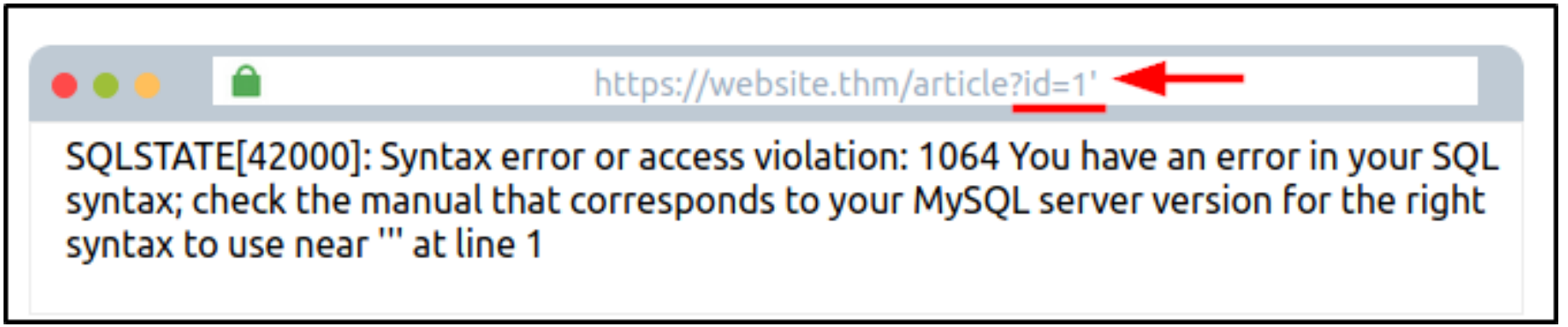
SQL Injection vulnerabilities can lead to sensitive data exposure, admin account takeover, webserver takeover, and more.

In-Band SQL Injection



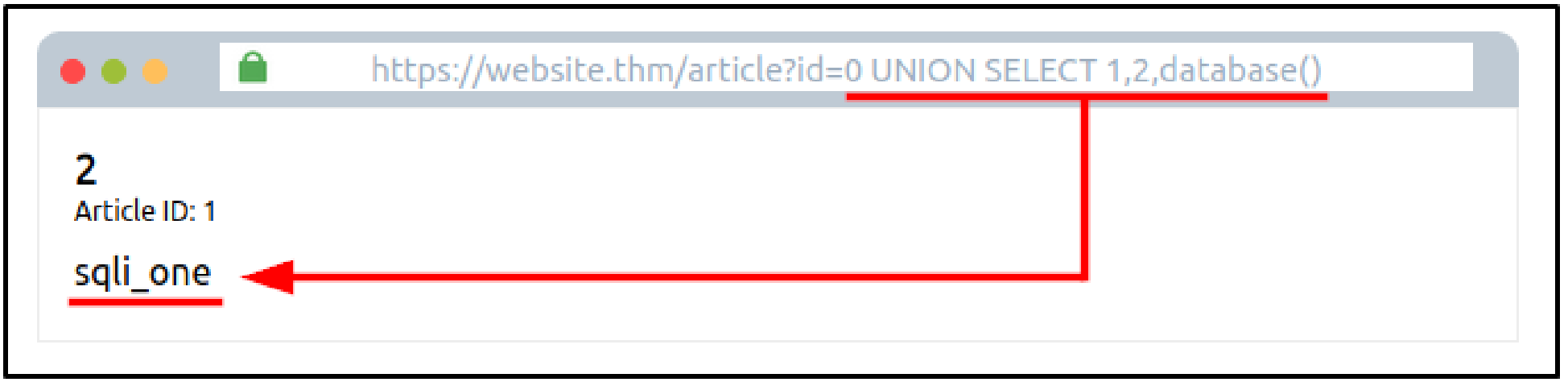
In-Band SQL Injection is SQL injection where the results of the injected query can be seen in the output of the web app. It is considered the easiest type of SQL injection to exploit.

Error-Based SQL Injection



Error-Based SQL Injection is a type of In-Band SQL Injection where error messages from the database software are returned to the web app interface.

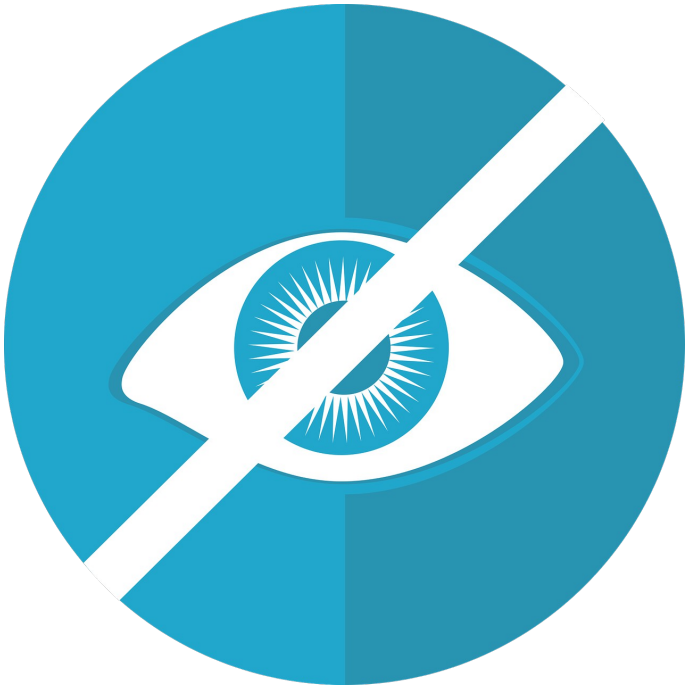
Union-Based SQL Injection



Union-Based SQL Injection uses the SQL UNION operator with a SELECT statement in order to output additional database information from the web app.

Blind SQL Injection

Blind SQL Injection is SQL injection where the error messages resulting from improper SQL queries has been disabled, but the requests are going through nonetheless.



Blind SQL Injection: Auth Bypass

Authorization Bypass is a type of Blind SQL Injection where insecurely written code allows the login of a user to a web app without the use of a proper username and / or password.

Blind SQL Injection: Auth Bypass

```
' or 1=1 --
```

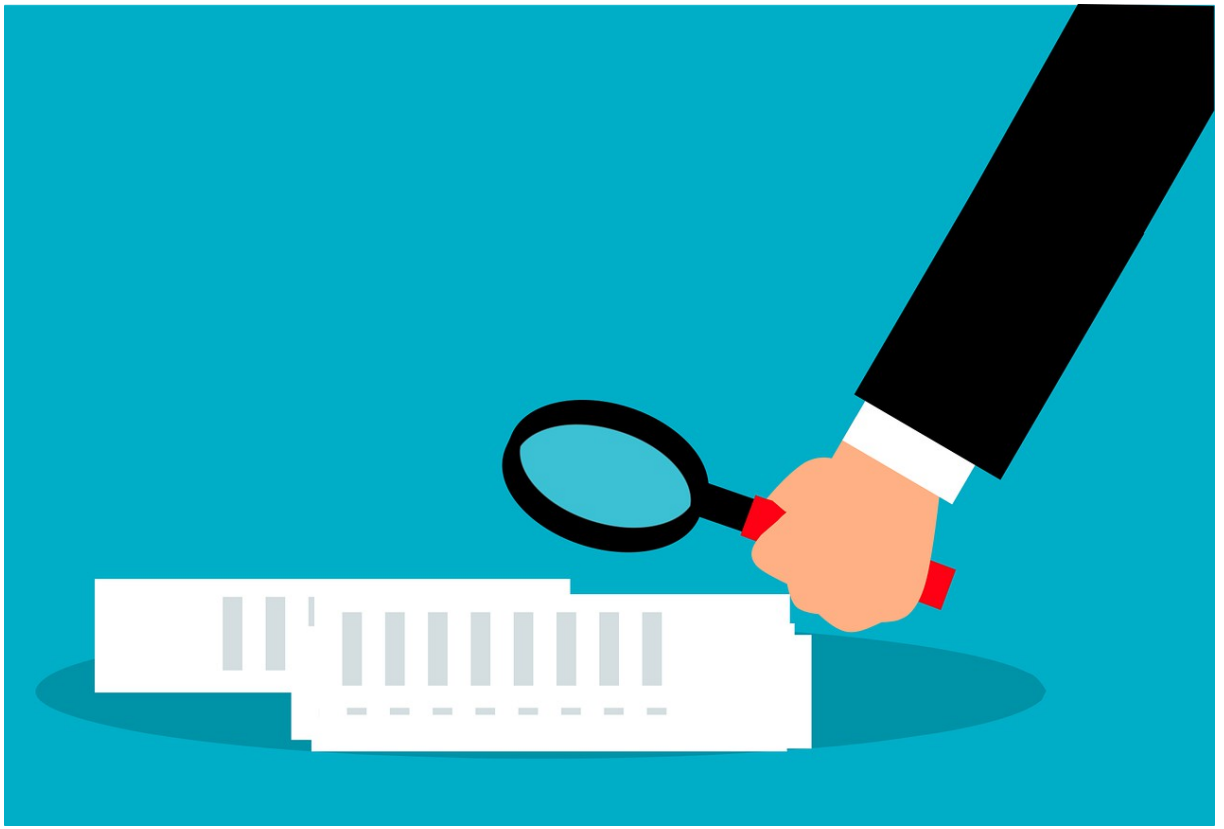
The most basic auth bypass SQL command is illustrated by the SQL command show above. Note that there is a space present in the command after the double dashes (--).

TryHackMe

Let's practice with TryHackMe at the following URL:

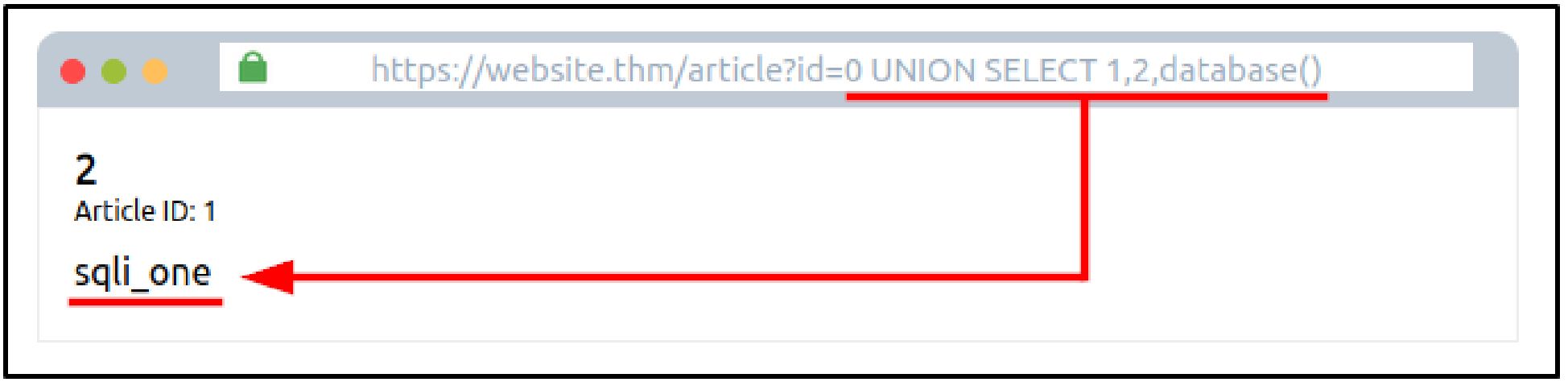
https://tryhackme.com/r/room/dvwa

Summary



Let's review the SQL concepts we learned in today's workshop:

Union-Based SQL Injection



We practiced doing SQL UNION injection attacks on both the DVWA app on TryHackMe and PicoCTF.

Blind SQL Injection: Auth Bypass

And we also practiced performing SQL login bypass attacks with the PicoCTF web app challenges.

Blind SQL Injection: Boolean Based

Boolean Based SQL Injection is a type of Blind SQL Injection where the only output that is returned after a SQL statement is whether the query returned true or false.

Blind SQL Injection: Time Based

Time Based SQL Injection is a type of Blind SQL Injection where we give the database software an instruction to return a delayed response, and if so, we know that the attack was successful.

Out-Of-Band (OOB) SQL Injection

Out-Of-Band (OOB) SQL Injection is a type of SQL injection where the output of any SQL queries can be passed to services outside of the web app's network.

What's Next?

In the next HackerFrogs AfterSchool web app hacking workshop, we'll be learning how to use Burpsuite, the industry-standard software for web app security testing.

Extra Credit

Looking for more study material on this workshop's topics?

See this video's description for links to supplemental documents and exercises!

Until Next Time, HackerFrogs!