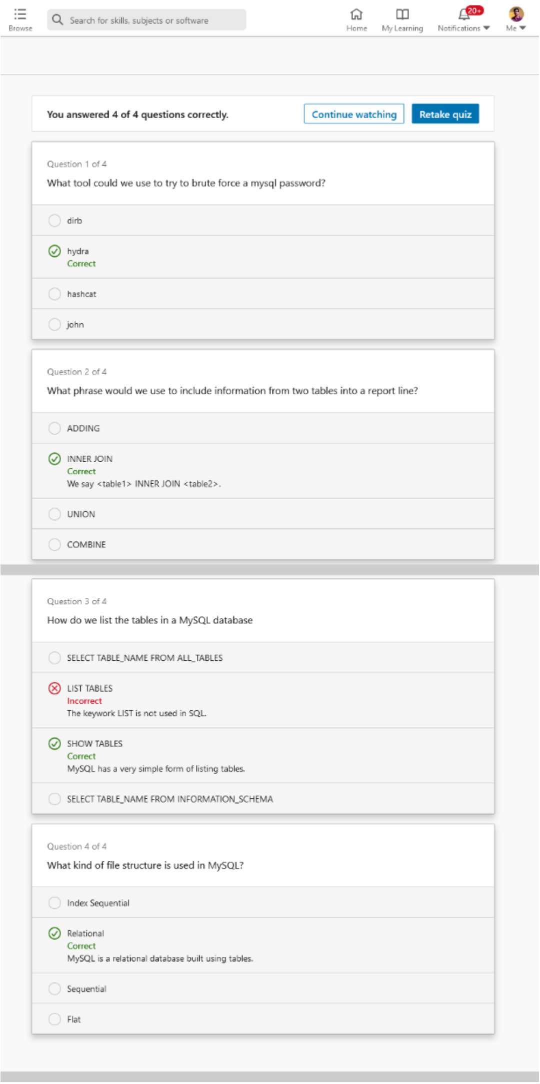
Introduction to the Course

With the dominance of cloud and software as a service delivery web portals are now the dominant means of accessing applications and are often supported by a backend SQL server. With the prevalence of SQL, adversaries will look for every opportunity to take advantage of unprotected SQL based applications to gain access to our information and systems. We need to protect our systems and that means understanding the basics of the SQL language and understanding how it can be used to penetrate our systems. This course teaches us how SQL injections work.

Learning objectives

- Injection in Mutillidae
- Injection in Microsoft & Oracle SQL Servers
- Cracking SQL hash
- SQL Injection via Burp Suite
- Defeating WAF
- SQLI Labs

Screenshots



You answered 4 of 4 questions correctly.

Question 1 of 4

What tool could we use to try to brute force a mysql password?

○ dirb

✓ hydra
Correct

○ hashcat

○ john

Question 2 of 4

What phrase would we use to include information from two tables into a report line?

○ ADDING

✓ INNER JOIN
Correct
We say <table1> INNER JOIN <table2>.

○ UNION

○ COMBINE

Question 3 of 4

How do we list the tables in a MySQL database

○ SELECT TABLE_NAME FROM ALL_TABLES

☒ LIST TABLES
Incorrect
The keywork LIST is not used in SQL.

✓ SHOW TABLES
Correct
MySQL has a very simple form of listing tables.

○ SELECT TABLE_NAME FROM INFORMATION_SCHEMA

Question 4 of 4

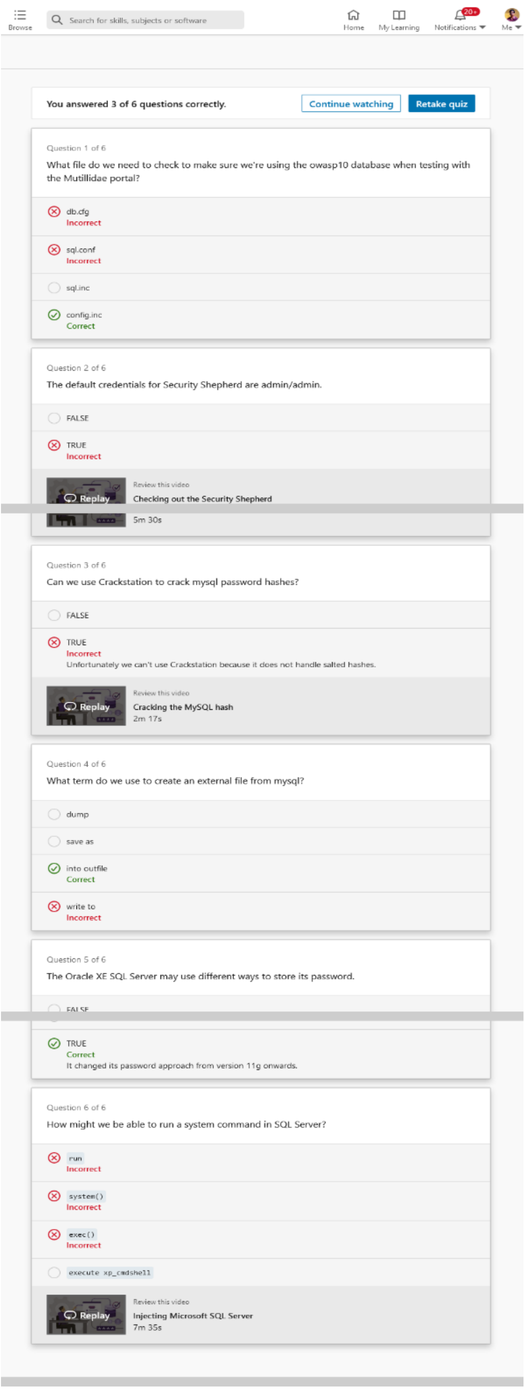
What kind of file structure is used in MySQL?

○ Index Sequential

✓ Relational
Correct
MySQL is a relational database built using tables.

○ Sequential

○ Flat



You answered 3 of 6 questions correctly.

Question 1 of 6

What file do we need to check to make sure we're using the owasp10 database when testing with the Mutillidae portal?

☒ db.cfg
Incorrect

☒ sql.conf
Incorrect

○ sql.inc

✓ config.inc
Correct

Question 2 of 6

The default credentials for Security Shepherd are admin/admin.

○ FALSE

☒ TRUE
Incorrect

Review this video
Checking out the Security Shepherd
5m 30s

Question 3 of 6

Can we use Crackstation to crack mysql password hashes?

○ FALSE

☒ TRUE
Incorrect
Unfortunately we can't use Crackstation because it does not handle salted hashes.

Review this video
Cracking the MySQL hash
2m 17s

Question 4 of 6

What term do we use to create an external file from mysql?

○ dump

○ save as

✓ into outfile
Correct

☒ write to
Incorrect

Question 5 of 6

The Oracle XE SQL Server may use different ways to store its password.

○ FALSE

✓ TRUE
Correct
It changed its password approach from version 11g onwards.

Question 6 of 6

How might we be able to run a system command in SQL Server?

☒ `run`
Incorrect

☒ `system()`
Incorrect

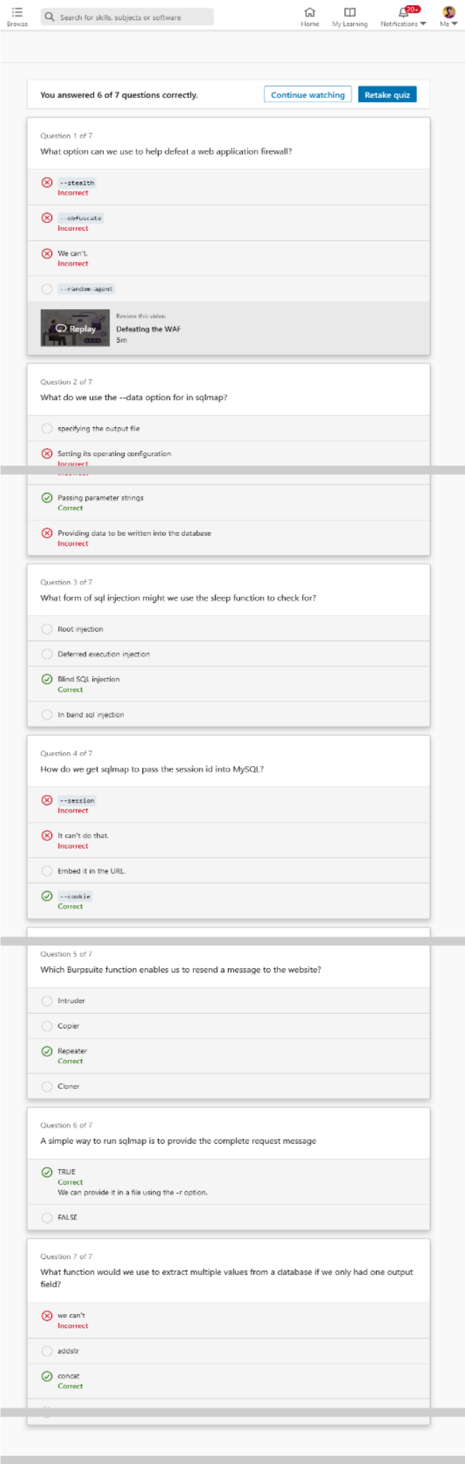
☒ `exec()`
Incorrect

○ `execute xp_cmdshell`

Review this video
Injecting Microsoft SQL Server
7m 35s

Figure: Section 01 – SQL Basics

Figure: Section 02- Testing for SQL Injections



You answered 6 of 7 questions correctly.

Question 1 of 7

What option can we use to help defeat a web application firewall?

⊗ `--stealth`
Incorrect

⊗ `--obfuscate`
Incorrect

⊗ We can't.
Incorrect

○ `--random-agent`

Review this video

Defeating the WAF

5m

Question 2 of 7

What do we use the --data option for in sqlmap?

○ specifying the output file

⊗ Setting its operating configuration
Incorrect

✓ Passing parameter strings
Correct

⊗ Providing data to be written into the database
Incorrect

Question 3 of 7

What form of sql injection might we use the sleep function to check for?

○ Root injection

○ Deferred execution injection

✓ Blind SQL injection
Correct

○ In band sql injection

Question 4 of 7

How do we get sqlmap to pass the session id into MySQL?

⊗ `--session`
Incorrect

⊗ It can't do that.
Incorrect

○ Embed it in the URL.

✓ `--cookie`
Correct

Question 5 of 7

Which Burpsuite function enables us to resend a message to the website?

○ Intruder

○ Copier

✓ Repeater
Correct

○ Cloner

Question 6 of 7

A simple way to run sqlmap is to provide the complete request message

✓ TRUE
Correct
We can provide it in a file using the -r option.

○ FALSE

Question 7 of 7

What function would we use to extract multiple values from a database if we only had one output field?

⊗ we can't
Incorrect

○ addstr

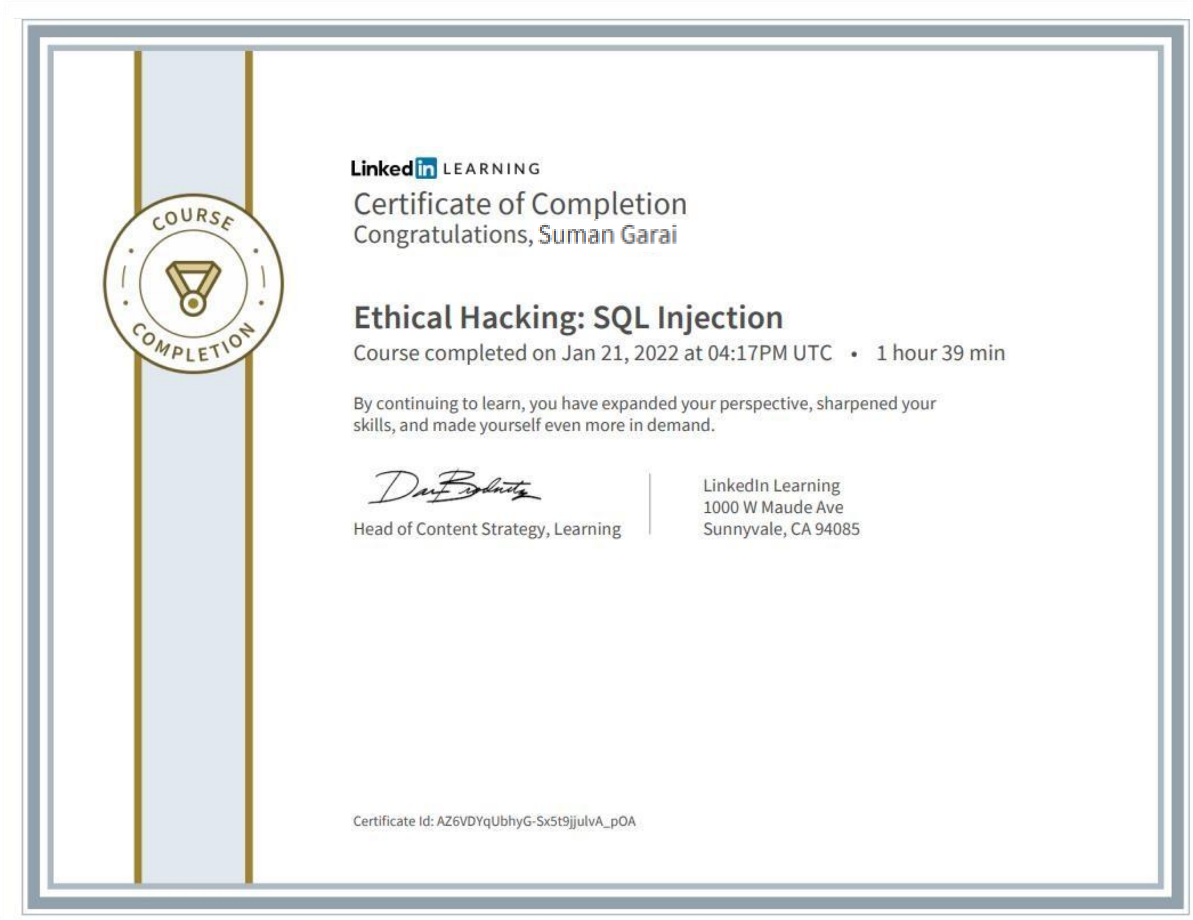
✓ concat
Correct

Figure: Section 03 – Automating SQL Injection Exploits

Conclusion

SQL injections are a common way to gain unauthorized access to web applications and extract data from them. In this course, instructor He shows you the SQL command language and how it is used by attackers to craft SQL Injections. He begins with commonly encountered relational databases and the basics of the SQL command language. Then he focuses on advanced SQL commands that may be used by attackers to achieve SQL injections. He explains how to use a simple Python script and how an SQL injection changes the backend SQL query. Then he demonstrates how SQL injections could be used to exploit some testing targets. He steps through the process of automating SQL injection exploits, then finishes with advice on how to continue to hone your skills as a penetration tester.

Certificate



COURSE COMPLETION

Linked in LEARNING

Certificate of Completion

Congratulations, Suman Garai

Ethical Hacking: SQL Injection

Course completed on Jan 21, 2022 at 04:17PM UTC • 1 hour 39 min

By continuing to learn, you have expanded your perspective, sharpened your skills, and made yourself even more in demand.

Head of Content Strategy, Learning

LinkedIn Learning
1000 W Maude Ave
Sunnyvale, CA 94085

Certificate Id: AZ6VDYqUbhyG-Sx5t9jjulvA_pOA