



**JAIN**  
DEEMED-TO-BE UNIVERSITY

SCHOOL OF  
COMPUTER  
SCIENCE AND IT

Department of  
**Bachelor of Computer Applications**

**Information Security & Mobile Applications – Section <A>**

**Ethical Hacking Fundamentals**  
Activity #01

**LinkedIn Learning Certification Course**  
*[Part-VI: SQL Injection]*

**Subject Code: 19BCA4C02**  
**Class: II<sup>nd</sup> Year II<sup>nd</sup> Semester**

Submitted On:

23-12-2022

By:

Suman Garai  
20BCAR0246

---

Signature

Faculty In-Charge:

Dr. Ajay Shriram

Khushwaha

---

Signature



## Certificate

This is to certify that Mr./Ms. Suman Garai with USN 20BCAR0246 has satisfactorily completed the Activity I Part 1 LinkedIn Course Name: SQL Injection Hours: 1 hour 39 minutes prescribed by Department of BCA, School of Computer Science & IT, Jain (Deemed-to-be-University), Bengaluru for the partial fulfilment of fifth semester BCA Degree Course in the year 2021-2022, and has secured \_\_\_\_\_ out of 10.

23-12-2022

Date of Submission

\_\_\_\_\_  
Signature of Student

A handwritten signature in blue ink, appearing to read 'S. K. Sharma', is written over a horizontal line.

\_\_\_\_\_  
Signature of Faculty  
In-Charge



**JAIN**  
DEEMED-TO-BE UNIVERSITY

SCHOOL OF  
COMPUTER  
SCIENCE AND IT

## Evaluation Criteria

Sr. No.	Criteria / Parameters	Total Marks	Marks Obtained
1	On-time submission Certification	05	
2	Certification of Completion	05	
3	Report (with Assessment Screenshots test attempted)	05	
4	Conclusion [ Minimum one page without any kind of plagiarism]	10	
	TOTAL	25	
	CONVERT	10	

## Table of Contents

Sl. No.	Title	Page No.
1	Introduction to the Course	5
2	Screenshots with name and section	6-7
3	Conclusion	8
4	Certificate	9

# 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

Search for skills, subjects or software

Home My Learning Notifications Me

You answered 4 of 4 questions correctly. [Continue watching](#) [Retake quiz](#)

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 keyword 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

Figure: Section 01 – SQL Basics

Search for skills, subjects or software

Home My Learning Notifications Me

You answered 3 of 6 questions correctly. [Continue watching](#) [Retake quiz](#)

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

[Replay](#) 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.

[Replay](#) 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()x  
Incorrect

☒ exec()x  
Incorrect

☐ sp\_execute\_external\_script

[Replay](#) Review this video  
Injecting Microsoft SQL Server  
7m 35s

Figure: Section 02- Testing for SQL Injections

Search for skills, subjects or software

Home My Learning Notifications Me

You answered 6 of 7 questions correctly. [Continue watching](#) [Retake quiz](#)


Question 1 of 7  
What option can we use to help defeat a web application firewall?

☒ --session  
Incorrect

☒ --confucate  
Incorrect

☒ We can't.  
Incorrect

☐ --randm-agent

 [Review this video](#)  
Defaulting the WAF  
See

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

☒ Resender  
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

☐ addslashes

☒ 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

