

32: Assisted Lab: Performing and Detecting SQLi

CySA+ (Exam CS0-003)



Congratulations, you passed!

Duration: 56 minutes, 39 seconds

✓ What user account name is not present in this SQLi result?

Score: 1

- ☐ admin
- ☐ Hack
- ☒ Morgan
- ☐ Bob
- ☐ Pablo
- ☐ Gordon

Congratulations, you have answered the question correctly.

✓ What is the first table name discovered from the DVWA database?

Score: 1

users

Congratulations, you have answered the question correctly.

✓ What is the second table name discovered from the DVWA database?

Score: 1

guestbook

Congratulations, you have answered the question correctly.

✓ Which of the following are column names from the users table of the dvwa database?
(Select eight column names)

Score: 1

- ☒ user_id
- ☒ avatar
- ☒ failed_login
- ☐ comment
- ☒ first_name
- ☒ last_login
- ☒ last_name
- ☐ name

- ☒ password
- ☐ permissions
- ☒ users

Congratulations, you have answered the question correctly.

☒ What is the HTTP referrer for this log record related to your first submission to the SQLi page of just the number '1'? Score: 1

- ☒ "GET /vulnerabilities/sqli/"
- ☐ "GET /vulnerabilities/sqli/?id=7&Submit=Sumbit# HTTP/1.1"
- ☐ "GET /vulnerabilities/xss_r/ HTTP/1.1"
- ☐ "GET /vulnerabilities/sqli/?id=1&Submit=Sumbit# HTTP/1.1"

Congratulations, you have answered the question correctly.

☒ What could be found in a website's access log as a representation of a space in an HTTP request? (Select 2) Score: 1

- ☒ + (a plus sign)
- ☐ %3c
- ☒ %20
- ☐ %22

Congratulations, you have answered the question correctly.

☒ What is the percent-encoding for a single quotation mark? Score: 1

- ☐ %3e
- ☐ %3a
- ☒ %27
- ☐ %21

Congratulations, you have answered the question correctly.

☒ Why is the octothorpe after the 'NULL' parameter used in this submitted SQLi statement? Score: 1

- ☒ end-of-line comment
- ☐ carriage return and line feed
- ☐ to append the command to the existing script statement
- ☐ retrieve certain records from one or more tables.

Congratulations, you have answered the question correctly.

☒ In SQLi, what is the most important character? Score: 1

- ☐ octothorp
- ☐ equals
- ☐ backslash
- ☐ asterisks

☒ single quote

Congratulations, you have answered the question correctly.

☒ What is the SQL expression used to combine instructions or operations?

Score: 1

- ☐ INSERT
- ☒ UNION
- ☐ SELECT
- ☐ FROM

Congratulations, you have answered the question correctly.

☒ What is SQL Injection?

Score: 1

- ☐ A form of file-sharing exploitation
- ☒ Injecting code or commands into a script to manipulate a DBMS
- ☐ A language used to access and manipulate databases.
- ☐ A type of database program.

Congratulations, you have answered the question correctly.

☒ Which of the following SQLi statements is used to return a result which includes the DBMS details?

Score: 1

- ☒ ' UNION SELECT @@version, NULL#
- ☐ ' UNION SELECT table_name, column_name FROM information_schema.columns#
- ☐ ' UNION SELECT table_schema, table_name FROM information_schema.tables#
- ☐ ' UNION SELECT user, password FROM users#

Congratulations, you have answered the question correctly.

☒ What evidence in a website's log is most clearly IoC observables related to SQLi?

Score: 1

- ☐ percent-encoding
- ☐ an HTTP referrer
- ☒ ORDER BY, UNION, SELECT, UPDATE, INSERT, DELETE, or DROP
- ☐ the HTTP response code of 200

Congratulations, you have answered the question correctly.