SQLI Labs Challenges

Ubuntu & MySQL

Challenge 1

http://192.168.2.11/sqli/sql1/ [Level: Basic]

- Bypass authentication and provide the flag id

Challenge 2

http://192.168.2.11/sqli/sql2/ [Level: Intermediate]

- Bypass authentication and provide the flag id

Challenge 3

http://192.168.2.11/sqli/sql3/ [Level: Advanced]

- Bypass authentication and provide the flag id

Challenge 4

http://192.168.2.11/sqli/sql4/ [Level: Basic]

- Identify the parameter vulnerable to SQL Injection
- What is the database version
- What is the username for database user?
- How many columns are returned in original SQL select statement?
- Provide the URL which will list all tables from back-end database
- What is the value of the flag stored in table secret (provide the URL which displays the flag)

Challenge 5

http://192.168.2.11/sqli/sql5/ [Level: Intermediate]

- Which parameter is vulnerable to SQL Injection?
- What is the current username?
- Which table contains column called Flag?
- Obtain the flag?

Challenge 6

http://192.168.2.11/sqli/sql9/ [Level: Advanced]

- Identify the database user and its privileges
- Where are the database passwords stored for database users?
- Obtain the password hashes for all users
- Identify what type of hash is it? What is the value of salt?
- What is the password for user root?
- Read the file /etc/passwd
- Create a file with your "name.txt" in http://192.168.2.11/sqli/sql9/tmp/
- What is the output of uname –a on database host?

Challenge 7

http://192.168.2.11/sqli/sql10/ [Level: Intermediate]

- Provide the url which displays content of /etc/passwd

Challenge 8

http://192.168.2.11/sqli/sql6/ [Level: Intermediate]

- Which parameter is vulnerable
- List techniques by which SQL Injection can be exploited
- Obtain the table which contains the column flag
- Obtain the flag

Challenge 9

http://192.168.2.11/sqli/sql7/ [Level: Advanced]

- Which parameter is vulnerable?
- Provide test case to confirm the SQL injection vulnerability

Challenge 10

http://192.168.2.11/sqli/sql8/ [Level: Advanced]

- Which parameter is vulnerable?
- Provide test case to confirm the SQL injection vulnerability.
- Obtain the database username and flag.

Challenge 11

http://192.168.2.11/sqli/gbk/ [Level: Advanced]

- Bypass Authentication and obtain the flag.

Challenge 12

http://192.168.2.11/sqli/admin1/ [Level: Advanced]

- Login as admin to obtain the flag.

Challenge 13

http://192.168.2.11/sqli/admin2/ [Level: Advanced]

- Login as admin to obtain the flag.

Ubuntu+Postgres

Challenge 14

http://192.168.2.11/sqli/sql13 [Level: Intermediate]

- Which parameter is vulnerable to SQL Injection?
- What is the database version?
- What is the database username?
- Which table stores the database schema?
- Provide a URL which lists all tables and the columns?
- Obtain the flag from backend database
- List privileges of current user?
- Where password hashes are stored (table, columns)?
- Comment on how database stores password hashes? What type of hash is it and what is the value of salt?
- Dump password hashes and crack hash for user postgres?
- Read file /etc/passwd (provide proof)
- Is it possible to execute OS code on the back-end database host? If so, list a technique by which it is possible?

IIS 7.5+ MS SQL 2008

Challenge 15

http://192.168.2.7/SQL1/ [Level: Basic]

- Provide the URL which displays SQL server version; provide a screenshot of the response.

Challenge 16

http://192.168.2.7/SQL2/ [Level: Basic]

- Provide the URL which displays SQL server username; provide a screenshot of the response.

Challenge 17

http://192.168.2.7/SQL3/ [Level: Intermediate]

- Which table(s) contain database schema?
- Provide a URL which displays list of all tables in the back-end database along with the respective columns.
- What are the columns within table secret?
- What is the password of user Alice?

Challenge 18

http://192.168.2.7/SQL10/ [Level: Intermediate]

- What is the SQL server username?
- Where does MS-SQL save password hashes for database users?
- In which format are password hashes stored?
- How can you obtain password hashes in hex format?
- What is the value of salt in password hash for user 'sa'?
- Obtain the password hashes for all user and the decrypted password?
- Does the current user have access to run xp_cmdshell?
- Is xp_cmdshell enabled?
- What are the contents of file c:\secret.txt
- Disable xp_cmdshell.

Oracle + Tomcat (jsp)

Challenge 19

http://192.168.2.12:8085/EmployeeSearchPortal/ [Level: Intermediate]

- What is the database version?
- What is the database username?
- What is the database service identifier (SID)?

- What are the column(s) in table SQLIROCKS?
- Obtain the flag?

Challenge 20

http://192.168.2.12:8085/EmployeeSearchPortal2/ [Level: Intermediate]

What is the database username?

Where are password hashes stored in Oracle database?

Obtain the password hashes?

What is the password for user SYS?

Challenge 21

Identify users with default/weak passwords on the oracle database listening on IP 192.168.2.12 [Level: Intermediate]

IP: 192.168.2.12

Port: 1521

SID: XE

- Login as user DBSNMP
- What are the current privileges of this user?
- Which privilege can be abused to read password hashes?
- Obtain and crack database password hashes for all users.

Challenge 22

Login to the oracle database based on the following information [Level: Intermediate]

Username: user1

Password: password1

IP: 192.168.2.12

Port: 1521

SID: XE

- List the permissions/privileges of current user.

- Escalate privileges and become DBA by exploiting a vulnerable procedure created by SYS user.

Challenge 23

Login to the oracle database based on the following information [Level: Intermediate]

Username: user2

Password: password2

IP: 192.168.2.12

Port: 1521

SID: XE

- List the permissions/privileges of current user.
- Escalate privileges and become DBA by exploiting a vulnerable trigger created by SYSTEM user.

Challenge 24

Login to the oracle database based on the following information [Level: Intermediate]

Username: user3

Password: password3

IP: 192.168.2.12

Port: 1521

SID: XE

- List the permissions/privileges of current user.
- Escalate privileges and become DBA by abusing the privileges granted to user.

Challenge 25

Login to the oracle database based on the following information [Level: Advanced]

Username: user4

Password: password4

IP: 192.168.2.12

Port: 1521

SID: XE

- List the permissions/privileges of current user.
- Escalate privileges and become DBA by abusing the privileges granted to user

Challenge 26

Login to the oracle database based on the following information [Level: Intermediate]

Username: DBA1

Password: password1

IP: 192.168.2.12

Port: 1521

SID: XE

- List the permissions/privileges of current user.
- Execute OS code and read the trophy file in c:\secret.txt.

Challenge 27

http://192.168.2.12:8085/EmployeeSearchPortal3/ [Level: Advanced]

What is the trophy stored in file c:\trophy.txt