PCS Lab 5: SQL Injection Instructions

Instructions

Read and follow the SEED lab instructions below, and answer the questions in the next page.

SEED Lab Instruction on SQLi:
http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Web/Web_SQL_Injection/Web_SQL_Injection.pdf

Some useful materials:

- Background Info: http://www.cis.syr.edu/~wedu/seed/Labs_16.04/Web/Web_SQL_Injection/
- OWASP page: https://www.owasp.org/index.php/SQL_Injection
- SQLi wiki by NetSPI: https://sqlwiki.netspi.com/
- A SQLi lab you could play with:https://github.com/Audi-1/sqli-labs

Submission

Due: May 1, 11:00 PM (EST)

Late submissions are accepted with 50% grading penalty within 24 hours of the due.
Submissions that are late for more than 24 hours will NOT be accepted.

Please submit your solution in PDF or image on https://www.gradescope.com/courses/38640.
Please choose the right page for your answer to every question.

Questions

Question 1: Please provide the names and NetIDs of your collaborator (up to 2). If you finished the lab alone, write None.

Collaboration Policy

1. **You can optionally form study groups consisting of up to 3 people per group (including yourself).**
2. **Everybody should write individually by themselves, and submit the lab reports separately. DO NOT copy each other's lab reports, or show your lab reports to anyone other than the course staff, or read other students' lab reports.**

Question 2 Please describe your observations of "Task 1: Get Familiar with SQL Statements", including necessary screenshots.

Question 3:

3.1 Please describe your observation of "Task 2.1: SQL Injection Attack from webpage", including

a. The exact content typed into USERNAME and PASSWORD
b. A screenshot showing that the user details of all users are successfully obtained.

3.2 Please describe your observation of "Task 2.2: SQL Injection Attack from command line"(The file you request should be home_unsafe.php instead of index.php here.), including

a. The exact command line(s) used for the attack.
b. The output of the command line.
c. Any screenshots if necessary for the description.

3.3 Why URL encoding is necessary in Task 2.2 but not necessary in Task 2.1?

3.4 Please describe your observation of "Task 2.3: Append a new SQL statement", including code and necessary screenshots.If you failed to append a new statement, explain why.

3.5 Would you be able to launch SQL injection by exploiting the `Password` field? Why?

3.6 As an attacker, you surprisingly discovered that another famous blog website "csrflabelgg.com" is also hosted on this server during further information gathering. They both use mysql and "csrflabelgg.com" is using database "elgg_csrf". Would you be able to steal the value of `__site_secret__ ` from table `elgg_csrfdatalists` in that database?
Please include:

a. The exact content typed into USERNAME and PASSWORD
b. The output of the successful attack.
c. Any screenshots if necessary for the description.

3.7 You know the table and column names that are used in your payload for 3.6 because you could get access to the server even before launching the attack. But think of yourself as a remote attacker, you could ONLY interact with the target server through the webpage. How would you find the table name is “elgg_csrfdatalists” and column names are “name” and “value” for database “elgg_csrf”? Would the `show tables` command work here? What would work here instead? Please include:

a. The exact content typed into USERNAME and PASSWORD
b. The output of the successful attack.
c. Explain why `show tables` work or doesn’t work here.
d. Any screenshots if necessary for the description.

Question 4.

4.1 Please describe your observations of "Task 3.1: Modify your own salary", including

a. The exact contents filled into each field.
b. Screenshots if necessary for the description.

4.2 Please describe your observations of "Task 3.2: Modify other people’ salary.", including

a. The exact contents filled into each field.
b. Screenshots if necessary for the description.

4.3 Please describe your observations of "Task 3.3: Modify other people’ password", including

a. The exact contents filled into each field.
b. Screenshot if necessary for the description.