

Fundamentals of Security in Ethical Hacking

DCS22104

Lesson 7: Script injection

Department of Computing

Course outline

Week	Topic
1	Introduction to ethical hacking and reconnaissance
2	Network enumerators and system vulnerabilities
3	Malware
4	Social engineering attacks
5	Hacking web servers and web applications
6	Session hijacking
7	Script injections
8	Hacking wireless network
9	Buffer overflow attacks
10	Cryptography
11	Evading IDS, firewall, and honeypot
12	Penetration testing

Assessments

#	Components	Marks(%)	Week
1	Test 1 (Topics 1 to 5)	10	DONE
2	Midterm examination	20	7
3	Test 2 (Topics 1 to 11)	20	12
4	Final examination	50	Exam week

Reviews on Lesson 6

Security flaws for a web server.

- a. Poor data validation.
- b. Insecure directory or in general direct object reference.
- c. Poor authentication.
- d. No security practices.
- e. Malware attacks.
- f. Leak of system information.
- g. Insecure login system.

Reviews on Lesson 6

Session hijacking is an approach to gain access and take control a victim's account through HTTP requests.

Two types of attacks for session hijacking.

- a. Passive attack, it waits for user's action.
- b. Active attack, it searches and steals user's credential.

Reviews on Lesson 6

Four ways to attack in session layer include

- a. Session side jacking (ARP proofing, e.g. AndroidSheep).
- b. Session attack using malware.
- c. Cross-site scripting (XSS).
- d. Session fixation. (Fake webpages, emails, etc.)

Data can be intercepted via **hub** or **switch** in a web system.

Reviews on Lesson 6

Three ways to prevent XSS attacks for the users.

- a. Logout from a private webpage to remove login credential left in the browser.
- b. Clear browser cache.
- c. Do not provide any sensitive information to an unknown or a suspicious website.

Reviews on Lesson 6

Three ways to prevent XSS attacks for the developers.

- a. Data validation,
- b. Reduce number of inputs, thus reduce number of points of attacks,
- c. Thoroughly test the web application to prevent any leak of system information.

Topic learning outcomes

- 1.Explain how SQL injection could alter database standard procedure.
- 2.Explain the important of database security.
- 3.Explain the technologies involved to prevent SQL injections.

Lesson 7: Lecture and lab sessions

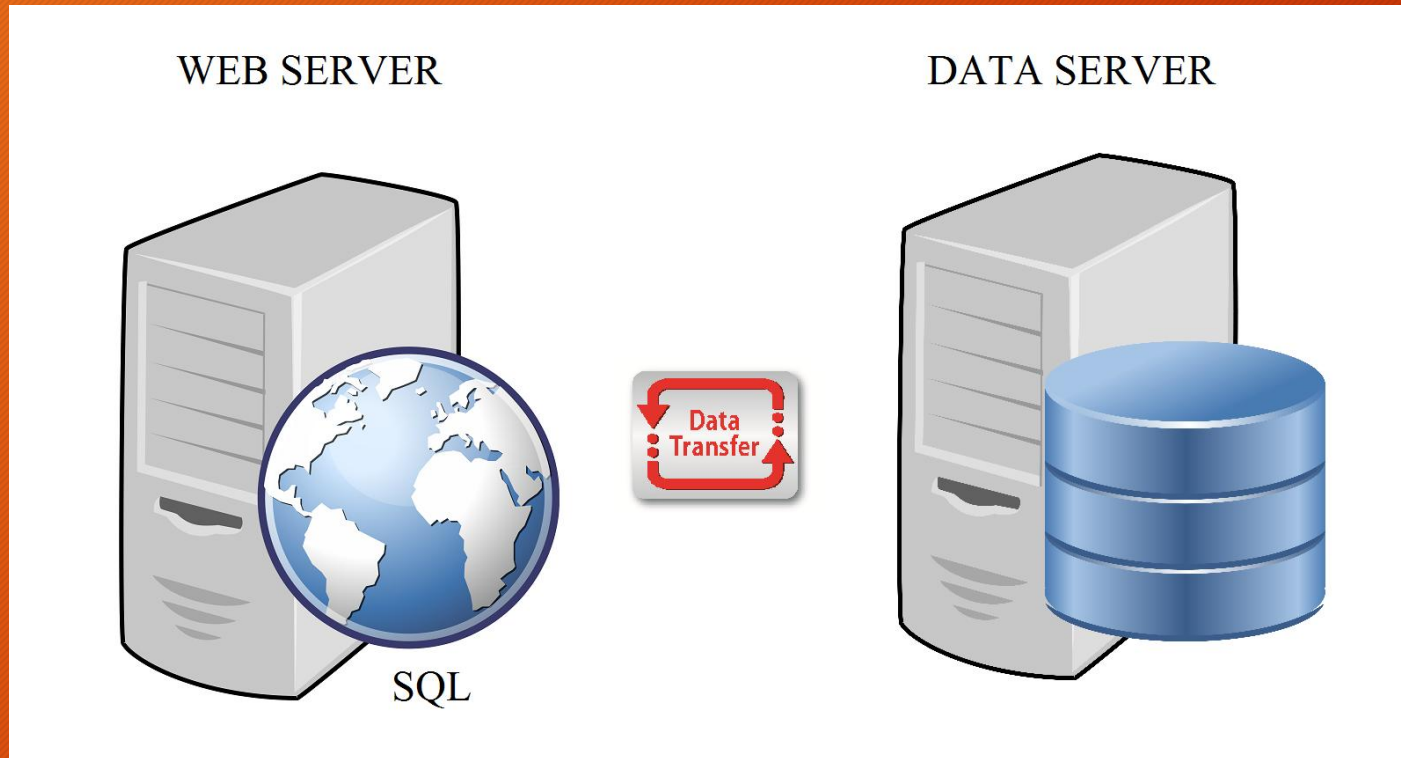
Start time	End time	Topics
1:00pm	1:30pm	Reviews on Lesson 6
1:30pm	2:00pm	Lecture 1: Introduction to SQL injection
2:00pm	2:15pm	Break time
2:15pm	2:45pm	Lecture 2: Data validation
2:45pm	2:50pm	References

Lecture 1: Introduction to SQL injections

SQL

- Sometimes refer to sequel.
- It stands for structured query language.
- It is a language that communicate with relational database management system (RDBMS).
- Data can be manipulated using SQL which included
 - (a) retrieve data,
 - (b) store data,
 - (c) delete data, and
 - (d) update data.


SQL in web architecture



SQL in web server

- SQL usually coded within a web server.
- Queries are sent to the database server via hypertext transfer protocol (HTTP).
- Also, data are fetched via HTTP in the record set format.

Use of SQL from the client-side

- An authorized user able to manipulate data through a webpage, which is a document object model (DOM) from a web browser.
- Unhandled SQL error sometimes will expose database information to the client.
- Example unhandled SQL error: 

- (a) `Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in /path/.../processsql.php on line 22.`
- (b) `SQLSTATE[HY000]: General error: 1 no such table: students.`
- (c) `Notice: Undefined variable: sqlString in C:\path\folder\sql.php on line 15`

Short-circuit evaluation

- Hacker could abuse the propositional logic to by pass security checks.
- Example SQL string as below:

```
SELECT * FROM users WHERE username= 'user' AND password='pw'
```

- Example crafted inputs from client-side:
- user: ' OR '1' = '1
- pw: ' OR '1' = '1
- Substituting the crafted inputs, the SQL string become

```
SELECT * FROM users WHERE username= '' OR '1'='1' AND  
password='' OR '1'='1'
```


Crafted malicious code

- More examples of crafted inputs from client-side:
- Empty version
- username: ' OR '' = '
- password: ' OR '' = '
- String injection
- username: ' OR 'anything' = 'anything
- password: ' OR 'anything' = 'anything

Exercise 1 (10 minutes)

1. What is SQL?
2. What is the purpose of SQL?
3. Write a version of SQL injection to bypass a login system.

Break time

Duration: 15 minutes.

Lecture 2: Data validation

Prepared SQL statements

- Also named as parameterized statement.
- It is a template to execute similar SQL statements.
- It could provide a layer of security where it separates data type of input data from SQL string.

- Prepare method:

```
$sqlString = prepare("SELECT * FROM users WHERE login:login AND password:password");
```

- Execute method:

```
$sqlString->execute(array(  
    ":login" => $user,  
    ":password" => $pw  
));
```

Escape key function

- To add escape keys to input data.
- To prevent unauthorized scripting languages entered into databases.
- Example addslashes() function:

```
SELECT * FROM users WHERE username= '\ ' OR '1'='1' AND password='\ ' OR '1'
```

```
SELECT * FROM users WHERE username= ' OR '1'='1' AND password=' OR '1'
```


Special character feature

- It is a function to translate any known special characters (i.e. HTML tags) into normal text.
- Apostrophe is used in PHP to prevent the misused of special characters, such as single quote (') in SQL statement, as below.

```
SELECT * FROM users WHERE `username` = ' OR '1'='1' AND `password`=' OR'1''
```
- Value shown in database with a single quotation mark will become ’.

Exercise 2 (10 minutes)

Give three approaches to prevent SQL injections.

References

- CEH course materials
- Goodrich, M (2010) *Introduction to Computer Security*, Addison Wesley, 1st Ed
- Purpura, P (2010) *Security: An Introduction*, CRC Press, 1st Ed
- Stallings, W (2007) *Computer Security: Principles and Practices*, Prentice Hall, 1st Ed
- Jacobson, D (2008) *Introduction to Network Security*, Chapman and Hall, 1st Ed
- Fischer, R (2008) *Introduction to Security*, Butterworth-Heinemann, 8th Ed