Text

Description automatically generated

**CENTRE FOR DIPLOMA STUDIES**

**UNIVERSITI TUN HUSSEIN ONN MALAYSIA (UTHM)**

**LAB 8**

**WEB SECURITY**

**COURSE CODE         DAT21303**

**COURSE NAME        WEB DEVELOPMENT**

**FACULTY                  CENTER OF DIPLOMA STUDY**

**DEPARTMENT OF INFORMATION TECHNOLOGY**

**STUDENT NAME     WAN MUHAMMAD ALIF FIRDAUS BIN WAN HANAPI**

**QAIREL QAYYUM BIN MUHAMAD RIDHUAN**

**NUM MATRIX AA210292**

**AA212363**

**SECTION                   6**

**LECTURE NAME    NOR NADHIA BINTI NOR AZMAN SUBRAMANIAM**

**SUBMIT DATE          8 JANUARY 2023**

**LABORATORY 8: Web Security**

|  |  |
| --- | --- |
| **Objective** | To enhance student knowledge related to web security mechanism and also to encourage web security awareness among students |
| **Required**  **Resources** | Macromedia Dreamweaver, Sublime Text, Bracket or if you are good enough just use text editor notepad. Xampp (used to dedicate your machine as server). |
| **References** | http://kr1.php.net/manual/en/language.functions.php  http://www.sqlcourse.com/table.html |
| **Date**  **Released** | 19/11/2017 |
| **Date**  **Submission** | 26/11/2017 |

Note: Do this Lab in a group of two people

**i. What is Web Security?**

Web sites are unfortunately prone to security risks. And so are any networks to which web servers are connected. Setting aside risks created by employee use or misuse of network resources, your web server and the site it hosts present you’re most serious sources of security risk. Web servers by design open a window between your network and the world. The care taken with server maintenance, web application updates and your web site coding will define the size of that window, limit the kind of information that can pass through it and thus establish the degree of web security you will have.

**ii. Several type of web attacks:**

❖ SQL Injection (SQLi)

❖ Cross-Site Scripting (XSS)

❖ Inclusion Vulnerabilities: Local File Inclusion (LFI) and Remote File Inclusion (RFI) ❖ Brute Force

DAT 32403 1st Semester Session 2017-2018

*DAT 32403 WEB PROGRAMMING HATTA & HALIM*

**iii. Why web security is crucial?**

An unprotected website is a security risk to customers, other businesses, and public/government sites. It allows for the spread and escalation of malware, attacks on other websites, and even attacks against national targets and infrastructure.

**Question 1:** Make a table and explain those attacks:

❖ SQL Injection (SQLi)

❖ Cross-Site Scripting (XSS)

❖ Inclusion Vulnerabilities: Local File Inclusion (LFI) and Remote File Inclusion (RFI) ❖ Brute Force

|  |  |  |  |
| --- | --- | --- | --- |
| **Type of Attacks** | **How the attacks occurs** | **Consequences** | **Prevention** |
| SQL Injection (SQLi) | SQL injection attacks are typically carried out by inserting malicious code into an application's input fields, such as a login form or a search box, that is then passed to a back-end database for processing. If the input is not properly sanitized and the database does not have sufficient defenses in place, the injected code can execute within the database and allow the attacker to access or modify sensitive data, or to execute other malicious actions. | Loss or theft of sensitive data: Attackers can use SQL injection to extract sensitive data, such as passwords, financial information, or personal information, from a database.  Compromise of entire systems: SQL injection attacks can be used to gain unauthorized access to a system and execute arbitrary code, allowing attackers to take control of an entire system. | To prevent SQL injection attacks, it is important to use prepared statements and parameterized queries, which are safe against such attacks, and to properly sanitize all user input to ensure that it does not contain any malicious code. It is also a good idea to use up-to-date security patches and to follow best practices for database security. |
| Cross-Site Scripting (XSS) | Reflected XSS: In a reflected XSS attack, the attacker injects malicious code into a website or web application by sending a request to the server with the code as a parameter. When the server processes the request and returns the response to the client, the code is executed by the victim's web browser. | Theft of sensitive information: XSS attacks can be used to steal sensitive information, such as login credentials or financial information, from victims.  Compromise of entire systems: XSS attacks can be used to execute arbitrary code on a victim's system, allowing attackers to take control of the system. | To prevent XSS attacks, it is important to properly sanitize all user input to ensure that it does not contain any malicious code. It is also a good idea to use up-to-date security patches and to follow best practices for web security. |
| Inclusion Vulnerabilities: Local File Inclusion (LFI) and Remote File Inclusion (RFI) | Local File Inclusion (LFI) occurs when an application includes local files from the server's file system. If an attacker can manipulate the input used to specify the file to be included, they may be able to access sensitive files on the server, such as configuration files or system logs.  Remote File Inclusion (RFI) occurs when an application includes files from a remote server. If an attacker can manipulate the input used to specify the file to be included, they may be able to execute arbitrary code on the server by including a malicious file from a remote location. | Compromise of entire systems: If an attacker is able to include and execute malicious code on a server via LFI or RFI, they may be able to take control of the system.  Loss or theft of sensitive data: LFI attacks may allow attackers to access sensitive files on the server, such as configuration files or system logs, which could contain sensitive information. | To prevent inclusion vulnerabilities, it is important to properly sanitize all user input to ensure that it does not contain any malicious code and to limit the types of files that can be included by the application. It is also a good idea to use up-to-date security patches and to follow best practices for web security. |
| Brute Force | A brute force attack is a type of cyber attack that involves attempting to guess a password or other piece of sensitive information by trying a large number of possible combinations. Brute force attacks can be used to gain unauthorized access to accounts, systems, or networks.  Brute force attacks can be carried out manually, but they are often automated using software tools that try a large number of combinations in a short period of time. The effectiveness of a brute force attack depends on the strength of the password being attacked, as well as the computational power of the attacker's system. | Loss or theft of sensitive information: If an attacker is able to gain access to an account, system, or network using a brute force attack, they may be able to access and steal sensitive information.  Compromise of entire systems: If an attacker is able to gain access to a system using a brute force attack, they may be able to take control of the system and execute arbitrary code. | To prevent brute force attacks and minimize the potential consequences, it is important to use strong passwords that are difficult for attackers to guess and to use two-factor authentication or other security measures to protect sensitive accounts. It is also a good idea to monitor for suspicious login attempts and to implement rate limiting to prevent attackers from attempting a large number of guesses in a short period of time. |

Thanks and Good Luck

DAT 32403 1st Semester Session 2017-2018