Module 14: SQL Injection

Objective

The objective of this lab is to provide expert knowledge on SQL Injection attacks and other responsibilities that include:

- Understanding when and how web application connects to a database server in order to access data
- Extracting basic *SQL Injection flaws* and *vulnerabilities*
- Testing web applications for *Blind SQL Injection vulnerabilities*
- Scanning web servers and analyzing the reports
- Securing information in web applications and web servers

Scenario

To be an expert *Penetration Tester* and *Security Administrator*, you must be able to perform SQL Injection, blind SQL Injection, extract Web application vulnerabilities and threats and server side technologies, use prepared statements, and bind variables.

As an expert *Ethical Hacker*, you must use diverse solutions, whitelisting input validation and escaping, and prepare statements with bind variables.

Virtual Machines

The following virtual machines are required for completion of this lab:

1. 2008 Server (10.10.10.1)
2. 2003 Server (10.10.10.61)
3. NAT

Exercise I: SQL Injection Attacks on MS SQL Database

Lab Scenario

*To be an Expert Penetration Tester and Security Administrator, you need to test web applications running on the **MS SQL Server database** for vulnerabilities and flaws.*

Lab Objectives

*The objective of this lab is to provide students with expert knowledge on SQL Injection attacks and to **analyze web applications for vulnerabilities**.*
In this lab, you will learn how to:

- *Log on without valid credentials*
- *Test for SQL Injection*
- *Create your own user account*
- *Create your own database*
- *Execute OS commands using XP command shell*
- *Directory listing*
- *Execute Denial-of-Service attacks*

1. **Switch to Windows 2003 Server (10.10.10.61)**

   Select **Windows 2003 Server** (10.10.10.61) from **Machines** section in the right pane of your lab environment.

2. **Log on to Windows 2003 Server Machine**

   Go to **Machine Commands** and select **Ctrl+Alt+Del**.

3. **Enter Credentials**

   In the log on box enter the following credentials and press **Enter**:
   User Name: **Administrator**
   Password: **Pa$$w0rd**

   You can use the **Paste Username** and **Paste Password** options from the **Machine Commands** menu to enter the user name and password.

4. **Logon to a Website Without Valid Credentials**

   Run this lab in Firefox, open a Firefox browser and type ***http://10.10.10.1/oldhouse*** in the address bar and press **Enter**.

   Click **LOGIN** to open the login page for the Old House Restaurant.

   The Home page of Old House Restaurant appears.

   It will not work in Internet Explorer.

5. **Login to the Site with SQL Injection Code**

   Assume that you are new to this site and have never registered with this website earlier.

   Now login with code **blah' or 1=1 --**

   Enter **blah' or 1=1 --** in the **Login name** field and enter any password in the **Password** field or leave the password field empty.

Click **Login** or press **Enter**

6. **Logged in with Fake Credentials**

   You are logged in to the website with a fake login. Your credentials are not valid, but you are logged in.

   Now you can browse all the web pages of the website as a registered member. You will get a **Logout** link at the right top corner of the screen.

7. **Creating Your Own User Account**

   Create user account using an SQL Injection query.

   Open a Firefox browser, type ***http://10.10.10.1/oldhouse*** and press **Enter**.

   The home page of Old House Restaurant appears. Click **LOGIN**.

8. **Enter the query**

   The Login page of Old House Restaurant appears.

   Enter the query **blah';insert into login values ('juggyboy','juggy123'); --** in the **Login name** field and enter any password in the **Password** field or leave the password field empty.

   After executing the query you will be redirected to the login page. This is normal.

   In the above query, **juggyboy** is the username, and **juggy123** is the password.

9. **Login Created Successfully**

   If no error message is displayed on the web page, it means that you have successfully created your login using SQL Injection query.

   To verify whether your login has been created successfully, go to the login page, enter **juggyboy** in the **Login name** field and **juggy123** in the **Password** field, and click **Login**.

   Username: **juggyboy**
   Password: **juggy123**

10. **Switch to Windows Server 2008**

    Switch to **Windows Server 2008** machine from **Machines** tab in the right pane of the lab environment.

11. **Logon to Windows Server 2008**

    Go to **Machine Commands** and click **Ctrl+Alt+Del**.

    In the log on box enter the following credentials and press **Enter**:
    User Name: **Administrator**
    Password: **Pa$$w0rd**

    Administrator is selected as User name by default, you just need to enter the Password.

    You can use the **Paste Username** and **Paste Password** options from **Machine Commands** menu to enter the user name and password.

12. **Open SQL server Management studio**

    Navigate to **Start** -> **All Programs** -> **SQL server Management studio**

13. **Connect to MS SQL Server 2008**

    Use the following credentials and click **Connect**.
    Login: **sa**
    Password: **qwerty@123**

14. **Check the Entries in Login Table**

    Expand the Databases node, **Databases** -> **oldhouse** -> **Tables**.

    Right-click on **dbo.Login** and select **Select Top 1000 Rows**.

    You can see the user name **juggyboy** that you have recently created in the **Results** pane.

15. **Create Your Own Database**

    Switch back to **Windows Server 2003** Machine.

    Open a web browser, type http://10.10.10.1/oldhouse in the address bar, and press **Enter**.

    The Home Page of Old House Restaurant appears.Click **LOGIN**.

16. **Enter the SQL Injection Code**

    In the **Login name** field, type ***blah';create database juggyboy; --***
    and leave the **Password** field empty. Click **Login.**

    In the above query, **juggyboy** is the name of the database.

No error message or any message displays on the web page. It means that the site is vulnerable to SQL Injection and a database with the name juggyboy has been created at the database server.

17. **Now Switch back to Windows Server 2008**

    Now switch back to Windows Server 2008.

    To check if the database is created in the webserver, navigate to **Start** -> **All Programs** -> **SQL server Management studio**.

    Connect to SQL Server 2008 R2 using following credentials:
    Login: **sa**
    Password: **qwerty@123**

    Expand the **Databases** node. You will see the **juggyboy** database.

18. **Executing OS Commands using XP Command Shell**

    Interacting with Operating System: Executing OS commands using XP command shell

    There are two ways to interact with the OS: One is reading and writing system files from disk, and the other is direct command execution via remote shell.

    Find passwords and execute command methods are restricted by the databases that are running privileges and permissions.

    Click **Start** --> **Administrative tools** --> **Services**. Right click on **SQL Server** service and select **Properties**.

    Go to **Log On t**ab, select the **Local System account** radio button and click on **Apply** and then **Ok**.

    Restart the **SQL Server** service.

19. **Execute ipconfig Command using xp_cmdshell**

    Swich to **Windows Server 2003** machine from machines tab from the right pane of the lab environment.

    Open a Web browser (Firefox) and type http://10.10.10.1/oldhouse in the address bar and press **Enter**.

    Click **Login** and enter the following code ***'; exec master..xp_cmdshell 'ipconfig > c:\inetpub\wwwroot\brown\ipconfig.txt';--*** in the **Login name** field and click on **Login** button or press **Enter**.

This query will run the **ipconfig** command in the Windows Server 2008 machine. The result of the **ipconfig** command will be saved **ipconfig.txt** file.

In the command shell query, **c:\inetpub\wwwroot\brown** is the location of the **ipconfig.txt** file.

20. **Switch to Windows Server 2008 Machine**

    Now switch to **Windows Server 2008** machine from **Machines** tab from the right pane of the lab environment.

    Navigate to **c:\inetpub\wwwroot\brown** folder and open the **ipconfig.txt** file. In this file you can see the IP configuration of the host system (Windows Server 2008 machine).

21. **Execute dir Command using xp_cmdshell**

    Switch to Windows Server 2003 machine.

    Open Oldhouse web page in firefox browser by typing http://10.10.10.1/oldhouse in the address bar and pressing **Enter**.

    Click on L**ogin** and enter the following code *'; exec master..xp_cmdshell 'dir c:\ > c:\inetpub\wwwroot\brown\c.txt';--* in the **Login name** field and click on **Login** or press **Enter**.

22. **Check Directory Information**

    Now type http://10.10.10.1/oldhouse/c.txt in the address bar of the firefox browser and press **Enter**.

    The page shows the directories of the Webserver (Windows Server 2008) machine.

23. **Use the xp_cmdshell to Extract IP Configuration**

    Use the **XP command shell** to extract IP configuration of a vulnerable web site using the **/all** option.

    Navigate to the Old House website's login page, enter the x-_cmdshell query ***'; exec master..xp_cmdshell 'ipconfig /all > c:\inetpub\wwwroot\brown\ipconfigall.txt';--*** in the login name field and click **Login**.

    In the above command shell query, **c:\inetpub\wwwroot\brown** is the location of the output file **ipconfigall.txt**.

    ipconfigall.txt file contains IP configuration infromation of the webserver (Windows Server 2008).

24. **Switch to Windows Server 2008 Machine**

    Now switch to the **Windows Server 2008** machine and navigate to the **c:\inetpub\wwwroot\brown** folder, and open the **ipconfigall.txt** file to view the IP configuration.

25. **Switch to Windows Server 2003 Machine**

    Now create tables in the website's database server.

    Navigate to the Old House web site login page, enter the xp_cmdshell query in the **Login name** field ***'; CREATE TABLE table1 (txt varchar(8000)); BULK INSERT table1 FROM 'test.txt'*** **--** click **Login**.

    If no error message displays, it means that the **xp_cmdshell** query has executed successfully.

26. **Switch to Windows Server 2008**

    To view the result of the executed command shell, go to **Microsoft SQL Server Management Studio** and expand the oldhouse database. In tables you will see table1, created by SQL Injection query.

    In old house database new table is created.

Lab Analysis

In this lab you have gained expert knowledge on SQL Injection attacks and analyzed web applications for vulnerabilities.

You have now:

- *Logged on without valid credentials*
- *Tested for SQL Injection*
- *Created your own user account*
- *Created your own database*
- *Executed OS commands using XP command shell*
- *Performed Directory listing*
- *Executed Denial-of-Service attacks*