HT102 – Application Vulnerability Assessment

Exercise 1 - Intercepting browser HTTP traffic

Description

- Open the web browser (Internet Explorer, Firefox, Chrome)
- Open Wireshark or Burp Suite
- If you use Burp Suite you have to modify the web browser connection properties and set the proxy web's address and port (e.g. address 127.0.0.1 port 8080)
- Try to navigate on a http page (e.g. BBC News Website) with the web browser and analyze the intercepted traffic with the application you choosed.

Exercise 2 - Intercepting HTTPS traffic with Burp Suite

Description

- Open the web browser (Internet Explorer, Firefox, Chrome)
- Modify the web browser connection properties and set the proxy web's address and port (e.g. address 127.0.0.1 port 8080)
- Open Burp Suite
- Try to navigate on a https page (e.g. BBC News Website) with the web browser and analyze the intercepted traffic.

Exercise 3 - Analysis of cookies delivery

Description

- Open the web browser (Internet Explorer, Firefox, Chrome)
- Modify the web browser connection properties and set the proxy web's address and port (e.g. address 127.0.0.1 port 8080)
- Open Burp Suite
- Try to navigate on a https page (e.g. Amazon UK) with the web browser and analyze cookies inside the intercepted traffic.

Exercise 4 - Analysis of a cross-domain communication with JavaScript

Description

- Open the web browser (Internet Explorer, Firefox, Chrome)
- Modify the web browser connection properties and set the proxy web's address and port (e.g. address 127.0.0.1 port 8080)
- Open Burp Suite
- Try to navigate on a http page that use a cross-domain communication (e.g. Example) and analyze HTTP header inside the intercepted traffic.

Exercise 5 - Identify and decode common types of encoding

Description

- Open the web browser (Internet Explorer, Firefox, Chrome)
- Modify the web browser connection properties and set the proxy web's address and port (e.g. address 127.0.0.1 port 8080)
- Open Burp Suite
- Try to navigate on different http pages with the web browser and analyze encoding used
- Burp Suite provides the "Decoder" functionality for common encoded data

Example:
URL encoding: Example
Base64: Sample HTTP Basic Authentication

Exercise 6 - Overview of Burp Suite tools

Description

- Open the web browser (Internet Explorer, Firefox, Chrome)
- Modify the web browser connection properties and set the proxy web's address and port (e.g. address 127.0.0.1 port 8080)
- Open Burp Suite
- Navigate over Burp Suite functionalities reading guide and trying to interact with the web browser

Exercise 7 - Google Hacking laboratory sessions

Description

Use the Google Advanced functionalities described in the "References" on different targets.

- Anonymous Googling
- Special Search Characters
- Trolling for Email Addresses
- Basic Site Crawling
- Intermediate Site Crawling
- Advanced Site Crawling

References

Google Hacking Guide

Exercise 8 - Using Bing Search to identify multiple virtual hosts

Description

- Open the web browser (Internet Explorer, Firefox, Chrome)
- Use the "ip:" function to search virtual hosts associated to an IP address (e.g. 83.221.106.128)

Exercise 9 - Fingerprinting web server with httprint

Description

Use HTTPrint tool (Windows version) to analyze a web server (e.g. www.apache.org)

Exercise 10 - Identify default resources using DirBuster and FuzzDB lists

Description

Use DirBuster and FuzzDB over the OwaspBWA Virtual Machine to discover wordpress application's paths (e.g. http://IP_OwaspBWA/wordpress)

Exercise 11 - Using BlindElephant to fingerprint a web application

Description

Use the BlindElephant tool (enclosed in your VM BlindElephant.py) to analyze one of the webapplication on the OwaspBWA running on the LAB Server (e.g. http://IP_OwaspBWA/wordpress)

Exercise 12 - Spidering a web app with Burp Suite Spider

Description

Use Burp Suite Spidering functionalities to navigate automatically the wordpress web application present on the OwaspBWA VM (http://IP_OwaspBWA/wordpress).

Exercise 13 - Web fuzzing with Burp Suite Intruder

Description

Use the four Burp Suite Intruder attacks:
- Sniper
- Battering RAM
- Pitchfork

- Cluster Bomb
over the DVWA web application present on the OwaspBWA VM.

Perform the attacks on the login form:

http://IP_OwaspBWA/dvwa/login.php

Exercise 14 – Web Application Flow-charting

Description

Find a real website (e.g. Amazon) and identify the different steps of a specific process (e.g. product payment).

Exercise 15 - Scanning a web application with nikto web scanner

Description

Use Nikto to perform a scan over a web application on OwaspBWA VM
(e.g. http://IP_OwaspBWA/wordpress)

Exercise 16 - Scanning a web application with SkipFish

Description

Use Skipfish to perform a scan over a web application on the OwaspBWA VM
(e.g. http://IP_OwaspBWA/wordpress)

Exercise 17 - Scanning a web application with Burp Suite Scanner Professional

Description

Uuse Burp Suite Pro to perform both an active and passive scan over a web application on OwaspBWA VM
(e.g. http://IP_OwaspBWA/wordpress).
Have a look about differences between these.

Exercise 18 - Scanning a web application with Tenable Nessus Scanner

Description

Use one of the tools present in your Kali VM (e.g. Nessus, w3af) to perfom a Web Scan over an application of OwaspBWA VM

Exercise 19 - Identify false positives and develop simple PoCs

Description

Using some of the vulnerabilities found in previous laboratories (e.g. Exercise 16, 17, 18), identify the existing ones and the false positives (if any). For the existing vulnerabilities, develop a simple proof of concept based on the scanner's output.

Exercise 20 - Risk evaluation of vulns identified by the scanner

Description

Use the OWASP Risk Rating methodology to rank some of the vulnerabilities found in previous laboratories (e.g. Exercise 16, 17, 18).