ICTACADEMY®

TATA STRIVE | Right Skills Bright Future

Web Server and Application Security

Web Application Vulnerability Scanning tools

March 2021

TATA TRUSTS

Ground Rules

1. For ease of conducting the session, we have disabled your microphones. Do keep your video turned on at all times.

2. Please raise any questions you may have through the chat.

3. Please confirm if you can see the presentation and the presenter clearly.

4. This is a 120-min long session. As we go through the session, I will take questions at the end of each concept and at the end of the session.

5. I will unmute the audio of participants volunteering for any activity.

Recap – M6 T8

Thus far, in the last module you've learned about:

- Mitigation/Recommendation
- Reporting – What should be part of the report

Recap – M6 T9

Thus far, in this topic you've learned about:

- Burp Suite
- Nikto
- CMSeeK
- WPScan

In case you have not gone through the Pre-study artefacts for this topic, please do it at the earliest.

Agenda

In today's session, you will learn about:

Vulnerability Scanning Tools namely

- Burp Suite
- Nikto
- CMSeeK
- WPScan

Source: Freepik

What is Burp Suite?

Created by fae frey
from Noun Project

Burp Suite Professional Tools

Burp Suite Professional contains the following tools:

- Proxy
- Spider
- Scanner
- Intruder
- Repeater
- Sequencer

Name of the Activity

Behind the Door Number

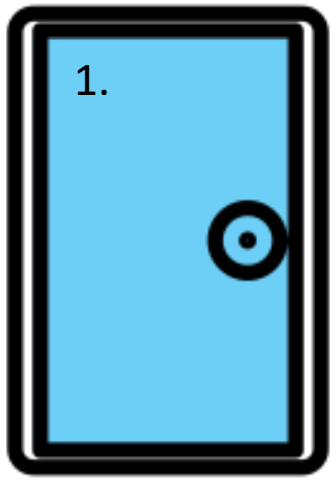
Instructions

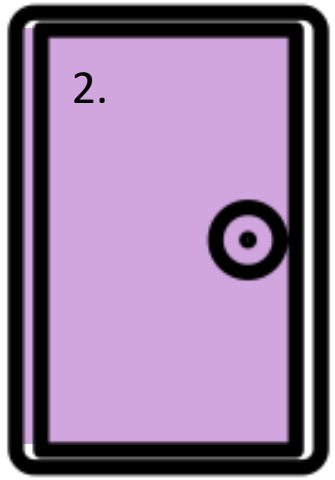
Mode: **In-session**

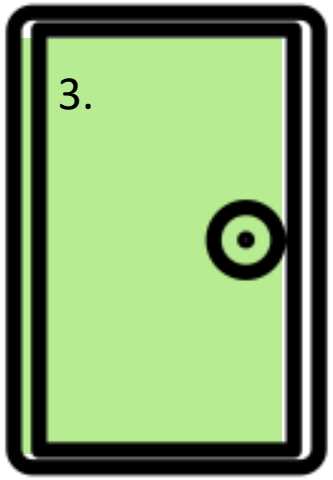
Duration: **5 minutes**

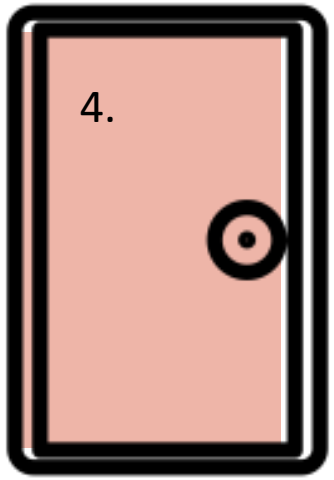
Materials Required: **None**

Activity – Behind the Door Number









Effectively Scanning Applications Using Burp

In order to obtain effective results from the Burp Scanner, it is recommended that you do the following:

- Turn “Intercept” (Proxy->Intercept) off within Burp.
- Configure your browser to use Burp as a proxy (Default port is 8080)
- Login to your web-application with the highest privileged account
- Right click on the Target URL (Target->site map) and click on “spider this host”
- Once spidering completes, Right click on the Target URL and click on “actively scan this host”.

Accuracy of Results

- While black-box testing tools can be of great assistance in uncovering major security vulnerabilities, it is important to understand that no tool can identify all vulnerabilities.
- Additionally, since these tools lack insight into the context of the application, false positives can be produced.
- The output of this tool should not be considered a comprehensive security assessment of your application; rather it should complement a thorough manual review.

Source: PortSwigger

Difference between Burp Community and Burp Pro

Burp Community	Burp Pro
HTTP(s) / WebSockets proxy and history	Web vulnerability scanner
Essential tools - Repeater, Decoder, Sequencer, and Comparer	Pro-exclusive BApp extensions
Burp Intruder (demo)	Orchestrate custom attacks (Burp Intruder - full version)
	Auto and manual OAST testing (Burp Collaborator)
	Automatically crawl and discover content to test

What is a False Negative?

Created by fae frey
from Noun Project

False Negatives

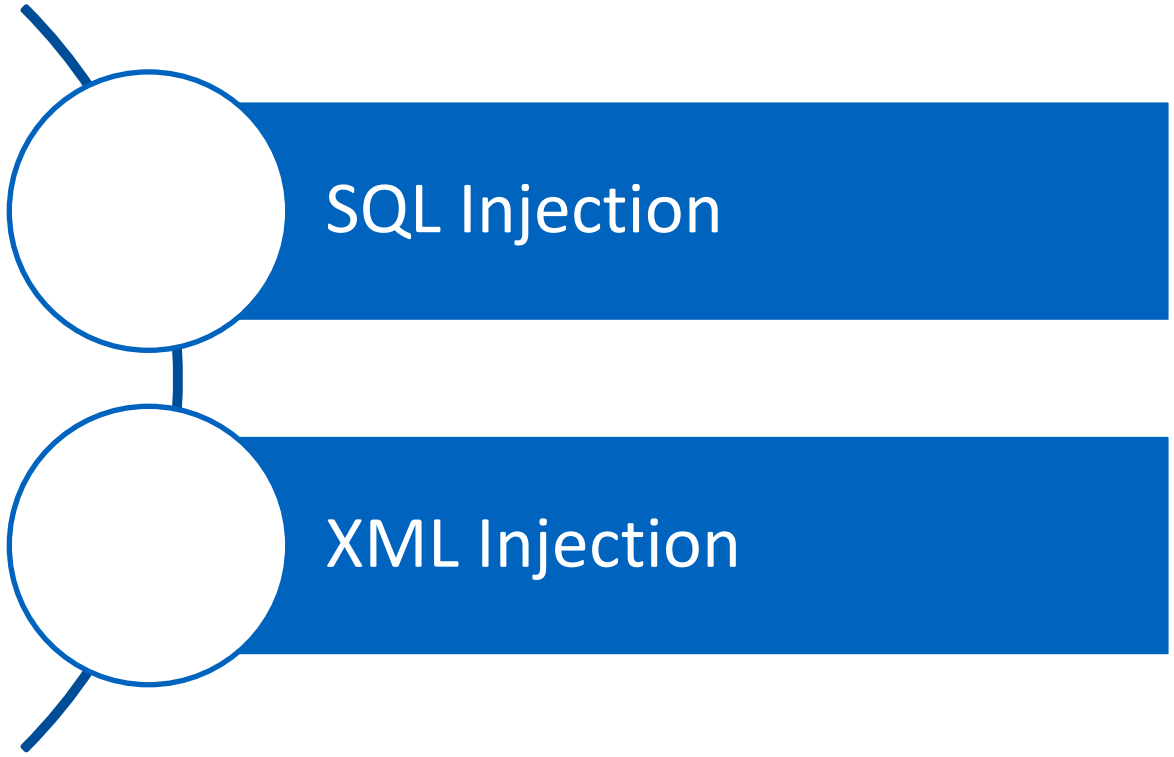
- A false negative occurs when a tool is not able to identify an existing bug.

Some vulnerabilities that Burp Suite may not identify are:

- Stored Cross-Site Scripting
- Cross-Site Request Forgery
- Session Hijacking/Fixation
- Weak Access Control Policy

False Positives

- A false positive occurs when a bug is flagged as being legitimate, which a tool misinterprets as being an actual issue.



Name of the Activity

Face Off

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

SQL Injection
v/s
XML Injection

What is Nikto?

Created by fae frey
from Noun Project

Nikto

- Nikto is a web application scanner that penetration testers, malicious hackers, and web application developers use to identify security issues on web apps.

- Nikto was originally written and maintained by Sullo, CIRT, Inc.

Source: Indusface

Nikto

Nikto allows pentesters, hackers and developers to examine a web server to find potential problems and security vulnerabilities, including:

- Server and software misconfigurations
- Default files and programs
- Insecure files and programs
- Outdated servers and programs

Source: DevOps

Features of Nikto

These are the main features of Nikto

- Nikto can be used to scan any web server (Apache, Nginx, Lighttpd, Litespeed, etc.)
- Scans for configuration-related issues such as open index directories
- SSL certificate scanning
- It has the ability to scan multiple ports on a server with multiple web servers running
- It can scan through a proxy and with http authentication

Source: SecurityTrails

Features of Nikto

During web app scanning, different scenarios might be encountered and Nikto supports a wide variety of options that can be implemented during such situations. The following is an overview of the included options in Nikto:

- -Cgidirs
- -config
- -host
- -id
- -list-plugins
- -Display
- -evasion
- -Format

Name of the Activity

Taboo

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Nikto Features

Display: Reference numbers are used for specification. The allowed reference numbers can be seen below:

- 1 – Show redirects
- 2 – Show cookies received
- 3 – Show all 200/OK responses
- 4 – Show URLs which require authentication
- D – Debug Output
- V – Verbose Output

Source: WebSecure

Nikto Features

-evasion: This option allows the use of reference numbers, multiple number references may be used:

- 1 – Random URI encoding (non-UTF8)
- 2 – Directory self-reference (/./)
- 3 – Premature URL ending
- 4 – Prepend long random string
- 5 – Fake parameter
- 6 – TAB as request spacer
- 7 – Change the case of the URL
- 8 – Use Windows directory separator ()

Source: CSO Online

Nikto Features

-Format: This option permits output/results to be saved to a file after a scan.

Valid formats are:

- csv – for a comma-separated lists
- htm – for an HTML report
- txt – for a text report
- xml – for an XML report

Source: EMK Technologies

The Output Format

The output format is Plugin name

-no404

-plugins

-port

-Pause

-timeout

-useproxy

-update

Name of the Activity

Behind the Door Number

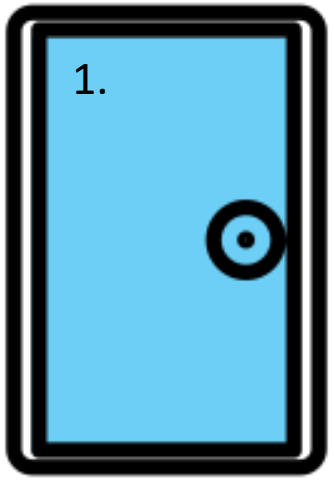
Instructions

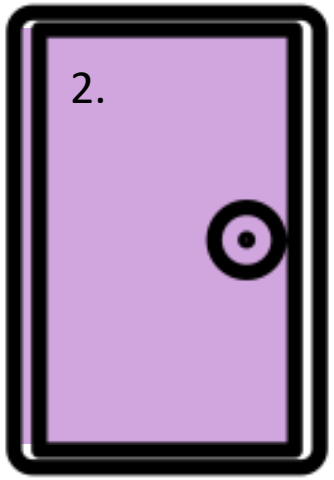
Mode: **In-session**

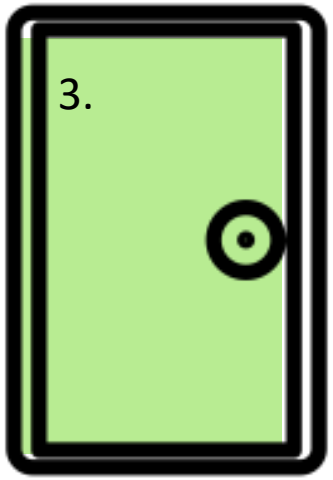
Duration: **5 minutes**

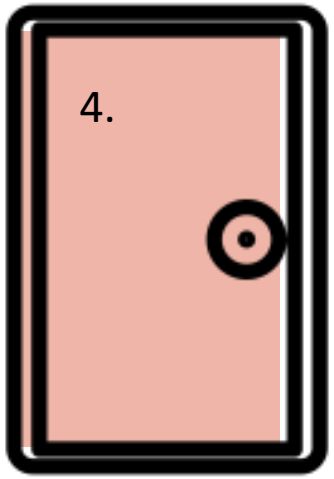
Materials Required: **None**

Activity – Behind the Door Number









Scanning Vulnerable Websites with Nikto

Using Nikto, scan http://webscantest.com which is a website intentionally left vulnerable for testing web application vulnerabilities. Typing on the terminal “nikto” displays basic usage options.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# nikto
- Nikto v2.1.6
---------------------------------------------------------------------------
+ ERROR: No host specified

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /directory
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
                + requires a value

        Note: This is the short help output. Use -H for full help text.

root@kali:~#
```

Source: InfoSec

Scanning Vulnerable Websites with Nikto

Once the scan is complete, results will be displayed in a format that closely resembles this screenshot

```
root@kali: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@kali: ~        root@kali: ~        root@kali: ~

root@kali:~# nikto -host http://webscantest.com
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          69.164.223.208
+ Target Hostname:    webscantest.com
+ Target Port:        80
+ Start Time:         2018-03-23 13:11:33 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.24
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to pro
tect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render t
he content of the site in a different fashion to the MIME type
+ Cookie TEST_SESSIONID created without the httponly flag
+ Cookie NB_SRVID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server leaks inodes via ETags, header found with file /robots.txt, fields: 0x65 0x52770f2
c6d6a3
+ "robots.txt" contains 4 entries which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (f
inal release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positive
s.
+ OSVDB-3092: /cart/: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /login.php: Admin login page/section found.
+ 7449 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2018-03-23 14:50:58 (GMT3) (5965 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~#
```

Source: InfoSec

Scanning Vulnerable Websites with Nikto

From the scan results, we can clearly see the identified issues along with their OSVDB classification. Nikto reveals:

- Server details such as the web server used,
- txt file with the number of present entries,
- Directory indexing that allows anyone browsing the website to access backend files and
- Apache web server default installation files.

Features of Nikto

- Nikto is an open-source vulnerability scanner, written in Perl and originally released in late 2001, that provides additional vulnerability scanning specific to web servers.
- It performs checks for 6400 potentially dangerous files and scripts, 1200 outdated server versions, and nearly 300 version-specific problems on web servers.
- If your victim's SIEM is active it is very easy to detect Nikto Scanning
- It is a free and open source scanning tool therefore IT enterprises can easily identify the security flaws in the organization and take necessary steps to shield and upgrade the system. The tool is able to find servers that were not developed by the enterprise.

What is CMSeeK?

Created by fae frey
from Noun Project

CMS Detection and Exploitation Tool

CMSeeK is a CMS detection and exploitation tool, written in Python3, capable of scanning numerous content management systems including WordPress, Joomla, Drupal, etc.

```
CMSEEK  by @r3dhax0r
        Version 1.1.1 Emporium

[+]  Tip: You can use cmseek via arguments as well check the help menu for more information  [+]

 Input    Description
=======  ============================
  [1]    CMS detection and Deep scan
  [2]    Scan Multiple Sites
  [3]    Bruteforce CMSs
  [U]    Update CMSeeK
  [R]    Rebuild Cache (Use only when you add any custom module)
  [0]    Exit CMSeeK :(

Enter Your Desired Option:
```

Source: CyberPunk

CMS Features

- CMSeeK can perform basic CMS detection: for plenty of different CMS (150+).
- Capable of advanced WordPress scans: plugins, user and theme enumeration; version and user detection (3 different detection modes); version vulnerabilities detection, etc.
- Beside WordPress version detection, it can detect Drupal version.

CMSeeK

CMS Detection and Exploitation suite

Source: CyberPunk

Detection Methods

- HTTP Headers
- Generator meta tag
- Page source code
- robots.txt

Source: CyberPunk

WPScan

- When using WPScan, scan the WordPress website for known vulnerabilities within the core version, plugins, and themes.

- One can also find out if any weak passwords, users, and security configuration issues are present. The database at wpvulndb.com is used to check for vulnerable software and the WPScan team maintains the ever-growing list of vulnerabilities.

WPScan

Source: WordPress

How to use WPScan

Updating WP Scan

- Open Terminal and change your directory to the wpscan folder we downloaded in the first tutorial

```
cd wpscan
```

- From this directory we can run a command to pull the latest update from Github, and then another command to update the database

```
git pull
ruby wpscan.rb --update
```

- You will see the WPScan logo and a note that the database update has completed successfully

```
alycia:wpscan artdecotech$ ruby wpscan.rb --update
_______________________________________________________________
        __          _______   _____
        \ \        / /   __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                         Version 2.8
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.
```

Source: Sucuri

Scanning for Vulnerabilities

- With a few commands, one can check the website for vulnerable themes, plugins, and users. From there one can take steps to secure the site by updating or disabling the security problems.

- WPScan commands will always start with ruby wpscan.rb followed by your website URL.

```
ruby wpscan.rb --url http://yourwebsite.com
```

Checking for Vulnerable Plugins

- Adding the **–enumerate vp** argument checks the WordPress website for vulnerable plugins.

```
ruby wpscan.rb --url http://yourwebsite.com --enumerate vp
```

- If vulnerable plugins are found you will see red exclamation icons and references to further information. Any vulnerable plugin should be replaced and removed if you cannot update it to patch the vulnerability.

Checking for Vulnerable Themes

- Similarly, adding **–enumerate vt** to the command checks the WordPress website for vulnerable themes.

```
ruby wpscan.rb --url http://yourwebsite.com --enumerate vt
```

- As with plugins, look for red exclamation icons and URLs with more information. Any vulnerable theme should be replaced and removed if you cannot update it to patch the vulnerability.

Checking User Enumeration

- To find out the login names of users on your WordPress website, we will use the argument –enumerate u at the end of the command.

```
ruby wpscan.rb --url http://yourwebsite.com --enumerate u
```

- If you have a Website Firewall or a plugin that stops WPScan, you may see an error.

```
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 2.8
          Sponsored by Sucuri - https://sucuri.net
   @_WPScan_, @ethicalhack3r, @erwan_lr, pvdl, @_FireFart_
_______________________________________________________________


    The target is responding with a 403, this might be due to a WAF
 or a plugin.
You should try to supply a valid user-agent via the --user-agent op
tion or use the --random-agent option
```

Source: Sucuri

Password Guessing

- When you have the wordlist file in the WPScan directory, you can add the –wordlist argument along with the name of the wordlist file.

```
ruby wpscan.rb --url http://yourwebsite.com --wordlist passwords.txt threads 50
```

Name of the Activity

Fill in the blanks

Instructions

Mode: **In-session**

Duration: **5 minutes**

Materials Required: **None**

Activity – Fill in the Blanks

1. In reference to Nikto, pentesters, hackers and developers are also allowed to specify the Intrusion Detection System evasion technique to use.

2. In regards to Password Guessing, If you have a list of passwords, WPScan can use the list to try logging in to each user account that it finds.

3. SQL Injection consists of insertion of a SQL query via the Input data from a user to the application.

4. CMSeeK is a CMS detection and exploitation tool, written in Python3, capable of scanning numerous content management systems

5. In WPScan, adding -enumerate vt to the command checks the WordPress website for vulnerable themes.

He Who Asks a Question

May Remain a Fool For Five Minutes

But, He Who Does Not Ask

Remains a Fool

Forever

Source: Freepik

Summary

In this session, you learnt about:

- Burp Suite
- Nikto
- CMSeeK
- WPScan

TATA STRIVE | Right Skills Bright Future

Skill Development Initiative of Tata Trusts

- www.tatastrive.com -