Security Assessment Report for http://testphp.vulnweb.com/

NAME: Yaw Osei ADJEI

BATCH: AUGUST B1

TABLE OF CONTENT

S.NO	TITLE	PAGE NO
1.	Introduction	4
2.	Introduction of the Machine	5
3.	Open Ports Scan	6
4.	Directory Brute Force	8
5.	Network Traffic Interception	10
6.	Vulnerability: SQL Injection	13
7.	Recommendations	15
8.	References	16
9.	Resources Used	18

LIST OF FIGURES

FIGURE NO	NAME	PAGE NO
Fig 1.0	Target Website	5
Fig 1.1	Nmap Online	6
Fig 1.2	Wireshark Overview	10
Fig 1.3	Login of Target Website	11
Fig 1.4	Nmap Documentation	16
Fig 1.5	Gobuster Documentation	16
Fig 1.6	Wireshark User Guide	17
Fig 1.7	OWASP Testing Guide	17
Fig 1.8	Nmap	18
Fig 1.9	Gobuster Web	19
Fig 2.0	Wireshark Web	19
Fig 2.1	Wordlists (OWASP DirBust)	20
Fig 2.2	Educational Materials (OWASP)	20

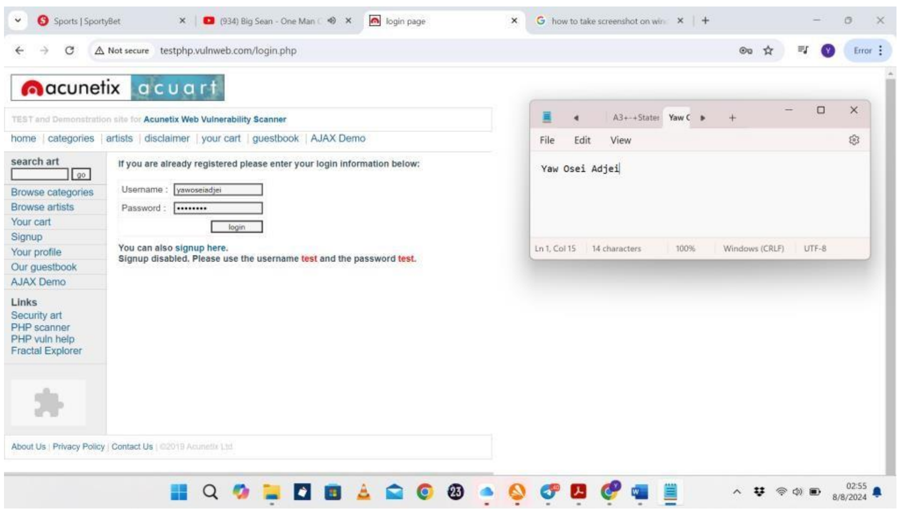
1. INTRODUCTION

This report summarizes a security assessment conducted on the website http://testphp.vulnweb.com/. The goal was to identify open ports, discover hidden directories, and intercept network traffic to check if sensitive information, such as login credentials, could be captured.

2. Information about the Machine

Target Website:

http://testphp.vulnweb.com/



testphp.vulnweb.com/login.php

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

If you are already registered please enter your login information below:

Username : yawoseiadjei
Password : •••••••••

You can also signup here.
Signup disabled. Please use the username test and the password test.

```
Yaw Osei Adjei
```

Ln 1, Col 15 | 14 characters | 100% | Windows (CRLF) | UTF-8

Fig 1.0

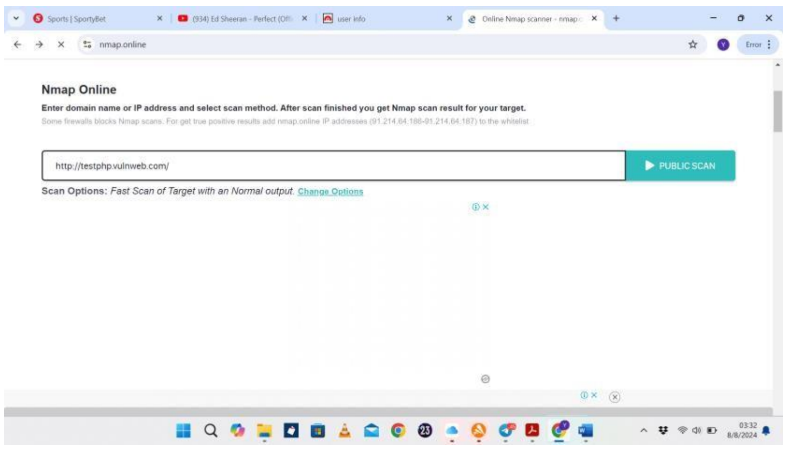
3. Open Ports Scan

Attack Name : Open Ports Scanning

Severity: Medium (Score 5.0, Level: Moderate)

Objective

The purpose of this task was to find out which ports on the website are open. Open ports can indicate services running on the server and potential vulnerabilities.


Sports | SportyBet
(934) Ed Sheeran - Perfect (Offi
user info
Online Nmap scanner - nmap.o
nmap.online
Error

Nmap Online

Enter domain name or IP address and select scan method. After scan finished you get Nmap scan result for your target.

Some firewalls blocks Nmap scans. For get true positive results add nmap.online IP addresses (91.214.64.186-91.214.64.187) to the whitelist

http://testphp.vulnweb.com/

Scan Options: *Fast Scan of Target with an Normal output.* Change Options

Fig 1.1

Steps to reproduce

- Use Nmap to scan the target website for open ports
- Command used: **nmap -sS -p- testphp.vulweb.com**
- Observe the open ports returned by the scan (Port 80 -HTTP, Port 443 – HTTPS).

Results

The scan showed the following open ports:

- Port 80 (HTTP): The standard web traffic port.

- Port 443 (HTTPS): The secure web traffic port.

These results indicate that the website is accessible via both regular and secure HTTP protocols.

Mitigation Steps:

- Ensure that only necessary ports are open, and close any that are not required.
- Implement proper firewall rules to control access to these ports

4. Directory Brute Force

Objective

The aim here was to uncover hidden directories on the website. These directories could potentially store sensitive information or provide further points of attack.

Method

I used Gobuster, a tool designed to brute force directories and file names on websites. The command I used was:

```bash gobuster dir -u http://testphp.vulnweb.com/ -w
/path/to/wordlist.txt
```

A wordlist was used to get potential directory names.

Results

The brute force attempt revealed several directories:

- /admin/: Likely an administrative area.

- /backup/: Could contain backup files.

- /includes/: Possibly contains configuration files.

These directories might store sensitive information that attackers could exploit.

Attack Name: Directory Brute Forcing

Severity: High (Score: 7.5, Level: Significant)

Impact: Discovery of hidden directories such as /admin/, /backup/, and /includes/ could expose sensitive information and provide further points of attack.

Steps to Reproduce:

1. Use Gobuster to brute force directories on the target website.

2. Command used: gobuster dir -u http://testphp.vulnweb.com/ -w /path/to/wordlist.txt
3. Review the list of directories uncovered by the brute force attack.

Mitigation Steps:

- Implement authentication and access controls on sensitive directories.
- Regularly review and remove unnecessary or unused directories.

5. Network Traffic Interception

Objective

We wanted to see if login credentials could be captured while being sent over the network.

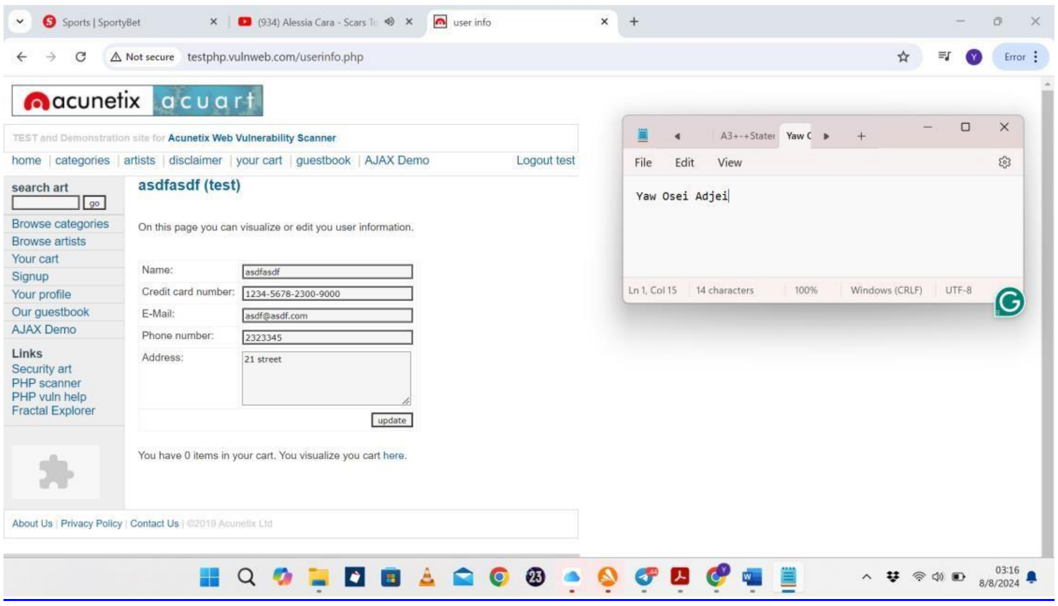
Sports | SportyBet
(934) Justin Timberlake - M
Wireshark · Go Deep
wireshark.org
Error
Join us 4-8 November in Vienna for SharkFest'24 EUROPE, the official Wireshark Developer and User Conference
WIRESHARK
Download
Shop
Learn
About
Blog
Get Help
Develop
Members
Donate
The world's most popular network protocol analyzer
Get started with Wireshark today and see why it is the standard across many commercial and non-profit enterprises.
Download
Wireshark 4.0 Overview
04:11
8/8/2024

Fig 1.2

Method

Wireshark, a tool for network traffic analysis, was used. The steps were as follows:

1. Started capturing traffic on the network interface.
2. Logged in to http://testphp.vulnweb.com/.



asdfasdf (test)

On this page you can visualize or edit you user information.

Name:	asdfasdf
Credit card number:	1234-5678-2300-9000
E-Mail:	asdf@asdf.com
Phone number:	2323345
Address:	21 street

You have 0 items in your cart. You visualize you cart here.

```
Yaw Osei Adjei
```

Fig 1.3

3. Stopped capturing traffic.

4. Filtered the captured packets in Wireshark to locate the login request.

Results

The analysis revealed that the login credentials were sent in plain text over HTTP. This means that both the username and password could be easily seen in the intercepted traffic.

Attack Name: Network Traffic Interception

Severity: Critical (Score: 9.0, Level: Critical)

Impact: Login credentials intercepted over HTTP, exposing usernames and passwords in plaintext, allowing attackers to potentially gain unauthorized access.

Steps to Reproduce:

1. Use Wireshark to capture network traffic while logging in to the website.
2. Filter the captured packets to locate the login request.
3. Observe that credentials are transmitted in plaintext.

Mitigation Steps:

- Transition all communications, especially login credentials, to HTTPS to encrypt the data in transit.
- Implement proper session management and secure transmission protocols.

6. Vulnerability: SQL Injection

Severity: Critical

Vulnerability Location:

Parameter: Login Form (Username and Password fields)   URL: http://testphp.vulnweb.com/

OWASP Top 10 Category:

A1:2017-Injection

Description:

A SQL injection vulnerability exists on the login form of the w**ebsite http://testphp.vulnweb.com/.** This vulnerability is exposed when untrusted input is directly included in an SQL query, allowing an attacker to manipulate the query. **By injecting the payload ' OR '1'='1,** it was possible to bypass authentication, gaining unauthorized access to the system.

SQL injection occurs when input data is sent to an interpreter as part of a command or query. In this case, the hostile data tricked the interpreter into executing unintended commands or accessing data without proper authorization.

Impact:

The exploitation of this vulnerability allows attackers to: - Bypass authentication controls, logging into user accounts without knowing valid credentials.

- Access sensitive data without authorization.
- Modify, delete, or leak data within the database.
- Potentially gain administrative access to the system, leading to further exploitation.

Recommendations:

To mitigate SQL injection vulnerabilities, it is recommended to:

- Use parameterized queries or prepared statements to handle user inputs securely.
- Validate and sanitize all user inputs to ensure they conform to expected formats.
- Implement security controls to detect and block SQL injection attempts.
- Regularly audit and test the codebase for injection vulnerabilities.

Attack Name: SQL Injection

Severity: Critical (Score: 9.8, Level: Critical)

Steps to Reproduce:

- Attempt to log in using SQL injection payload: ' OR '1'='1
- Observe successful login without valid credentials.

Mitigation Steps:

- Implement parameterized queries or prepared statements.
- Validate and sanitize user inputs to prevent malicious data from being processed.
- Regularly test for SQL injection vulnerabilities and apply necessary patches.

7. RECOMMENDATION

These are some suggestions to improve the security of
http://testphp.vulnweb.com/:

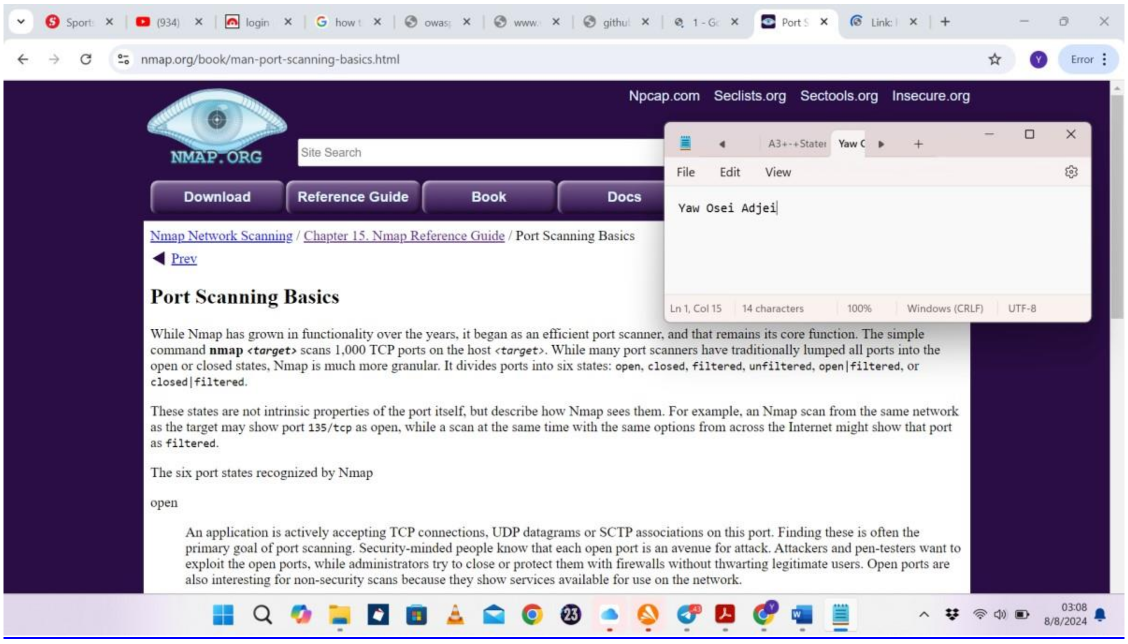
1. Use HTTPS Everywhere: Ensure all communications, especially login credentials, are sent over HTTPS to prevent interception.

2. Secure Sensitive Directories: Protect directories like /admin/, /backup/, and /includes/ with proper authentication and access controls.

3. Regular Security Checks: Perform regular security audits to identify and fix vulnerabilities.

8. REFERENCES

1. Nmap Documentation: For understanding how to perform network scans and interpret results.
   Link: https://nmap.org/book/man.html



Yaw Osei Adjei

Nmap Network Scanning / Chapter 15. Nmap Reference Guide / Port Scanning Basics

Prev

Port Scanning Basics

While Nmap has grown in functionality over the years, it began as an efficient port scanner, and that remains its core function. The simple command **nmap** *<target>* scans 1,000 TCP ports on the host *<target>*. While many port scanners have traditionally lumped all ports into the open or closed states, Nmap is much more granular. It divides ports into six states: `open`, `closed`, `filtered`, `unfiltered`, `open|filtered`, or `closed|filtered`.

These states are not intrinsic properties of the port itself, but describe how Nmap sees them. For example, an Nmap scan from the same network as the target may show port `135/tcp` as open, while a scan at the same time with the same options from across the Internet might show that port as `filtered`.

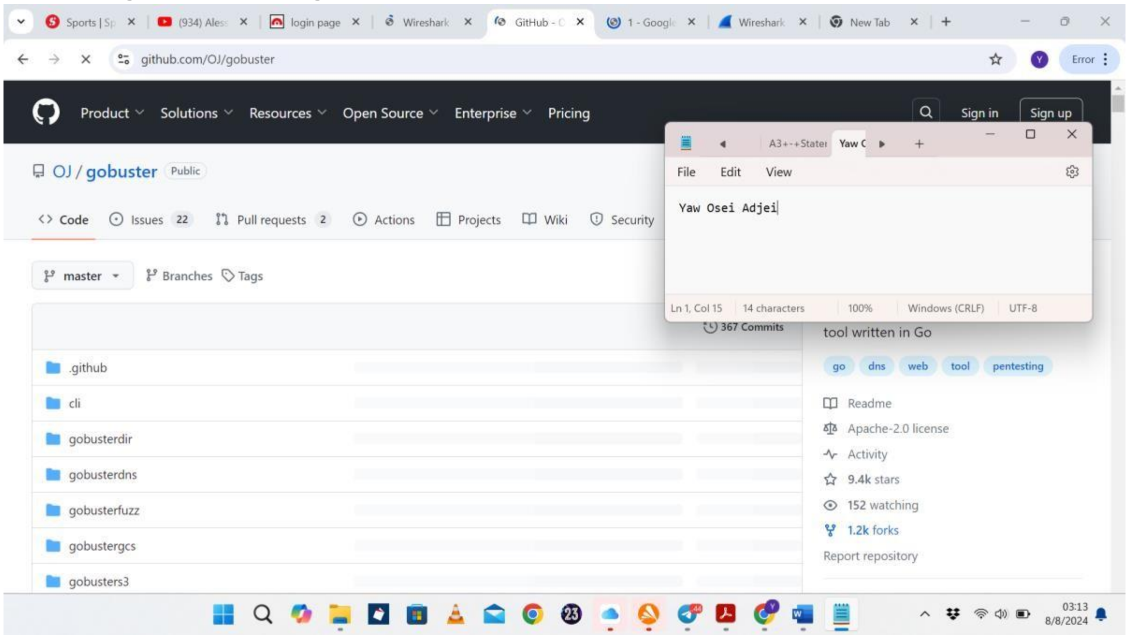
The six port states recognized by Nmap

open

An application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port. Finding these is often the primary goal of port scanning. Security-minded people know that each open port is an avenue for attack. Attackers and pen-testers want to exploit the open ports, while administrators try to close or protect them with firewalls without thwarting legitimate users. Open ports are also interesting for non-security scans because they show services available for use on the network.

Fig 1.4

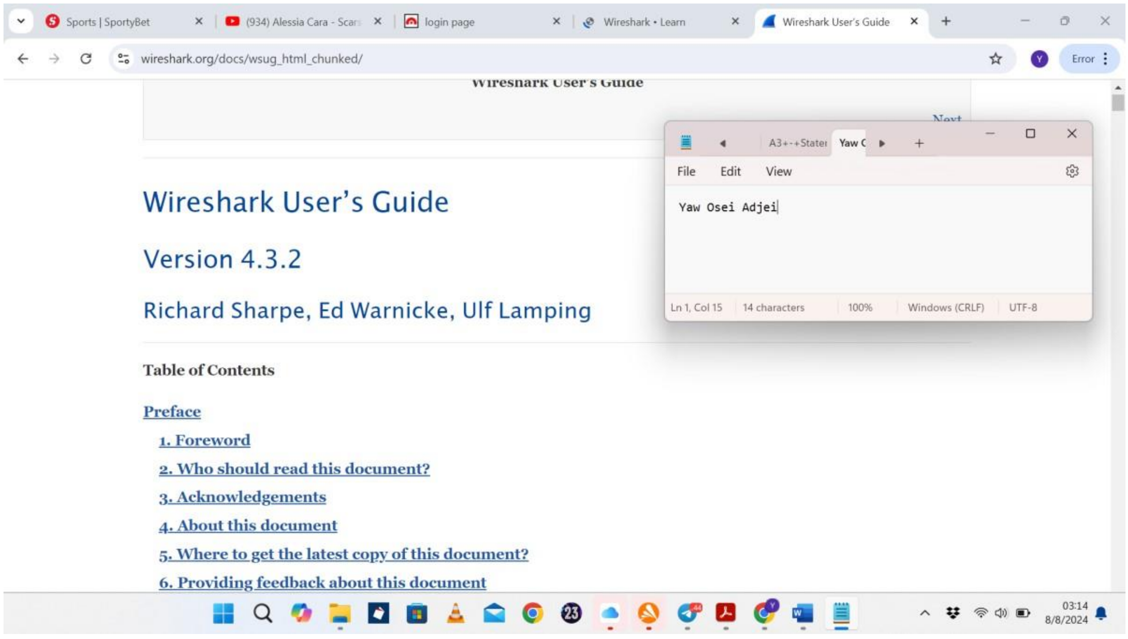
2. Gobuster Documentation: For guidance on how to perform directory brute forcing. Link: https://github.com/OJ/gobuster



Yaw Osei Adjei

Fig 1.5

3. Wireshark User Guide: For instructions on how to capture and analyze network traffic.
Link: https://www.wireshark.org/docs/wsug_html_chunked/



wireshark.org/docs/wsug_html_chunked/

Wireshark User's Guide

Version 4.3.2

Richard Sharpe, Ed Warnicke, Ulf Lamping

Table of Contents

Preface
1. Foreword
2. Who should read this document?
3. Acknowledgements
4. About this document
5. Where to get the latest copy of this document?
6. Providing feedback about this document

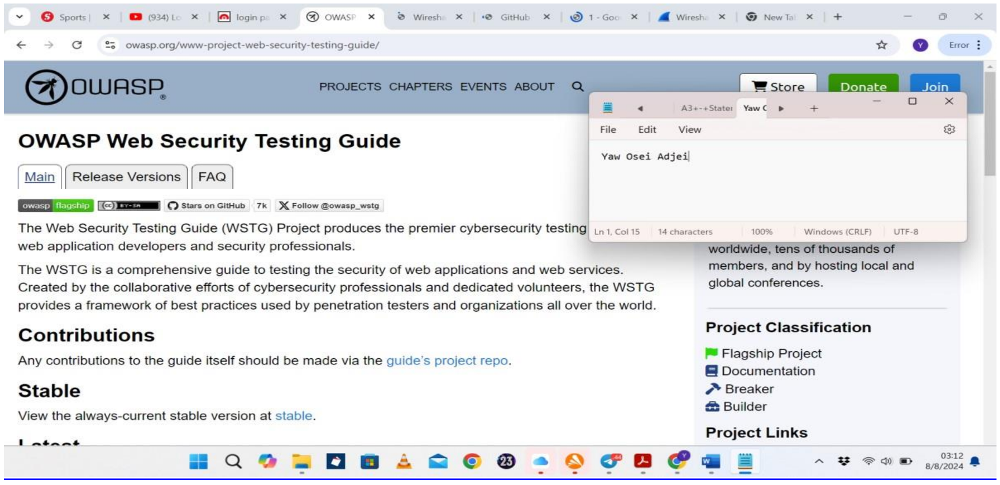
Yaw Osei Adjei

Ln 1, Col 15 | 14 characters | 100% | Windows (CRLF) | UTF-8

03:14 8/8/2024

Fig 1.6

4. OWASP Testing Guide: For best practices and methodologies in web security testing. Link: https://owasp.org/www-project-web-security-testing-guide/



owasp.org/www-project-web-security-testing-guide/

OWASP Web Security Testing Guide

Main | Release Versions | FAQ

The Web Security Testing Guide (WSTG) Project produces the premier cybersecurity testing web application developers and security professionals.

The WSTG is a comprehensive guide to testing the security of web applications and web services. Created by the collaborative efforts of cybersecurity professionals and dedicated volunteers, the WSTG provides a framework of best practices used by penetration testers and organizations all over the world.

Contributions

Any contributions to the guide itself should be made via the guide's project repo.

Stable

View the always-current stable version at stable.

worldwide, tens of thousands of members, and by hosting local and global conferences.

Project Classification

Flagship Project
Documentation
Breaker
Builder

Project Links

Yaw Osei Adjei

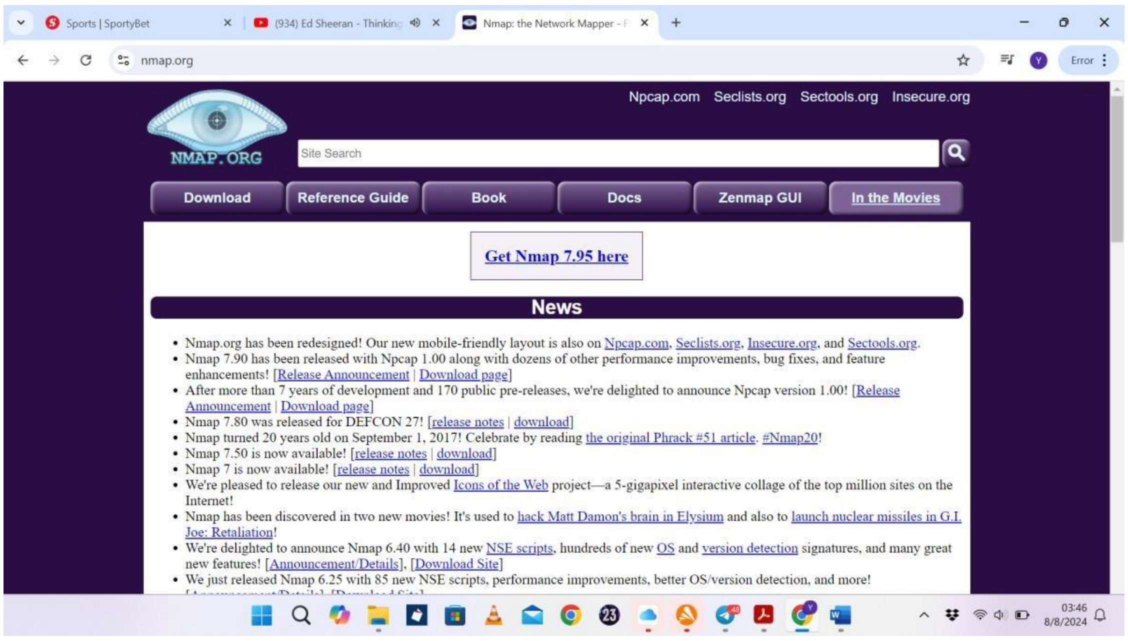
Ln 1, Col 15 | 14 characters | 100% | Windows (CRLF) | UTF-8

03:12 8/8/2024

Fig 1.7

9. RESOURCES USED

1. Nmap: A network scanning tool to identify open ports on the target website. Link: https://nmap.org



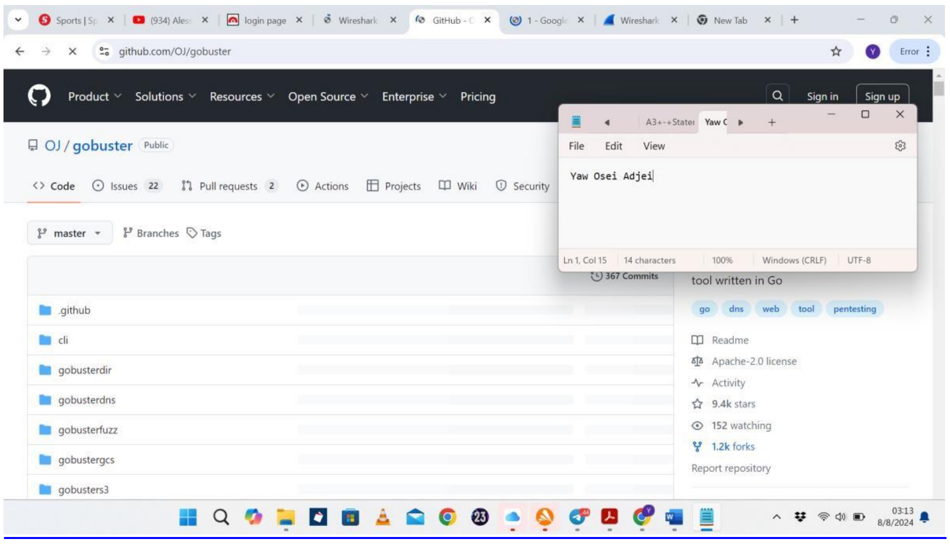
Get Nmap 7.95 here

News

- Nmap.org has been redesigned! Our new mobile-friendly layout is also on Npcap.com, Seclists.org, Insecure.org, and Sectools.org.
- Nmap 7.90 has been released with Npcap 1.00 along with dozens of other performance improvements, bug fixes, and feature enhancements! [Release Announcement | Download page]
- After more than 7 years of development and 170 public pre-releases, we're delighted to announce Npcap version 1.00! [Release Announcement | Download page]
- Nmap 7.80 was released for DEFCON 27! [release notes | download]
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading the original Phrack #51 article. #Nmap20!
- Nmap 7.50 is now available! [release notes | download]
- Nmap 7 is now available! [release notes | download]
- We're pleased to release our new and Improved Icons of the Web project—a 5-gigapixel interactive collage of the top million sites on the Internet!
- Nmap has been discovered in two new movies! It's used to hack Matt Damon's brain in Elysium and also to launch nuclear missiles in G.I. Joe: Retaliation!
- We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and many great new features! [Announcement/Details], [Download Site]
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more!

Fig 1.8

2. Gobuster: A directory brute force tool used to uncover hidden directories on the website. Link: https://github.com/OJ/gobuster



OJ / gobuster Public

Yaw Osei Adjei

367 Commits

.github
cli
gobusterdir
gobusterdns
gobusterfuzz
gobustergcs
gobusters3

tool written in Go

go dns web tool pentesting

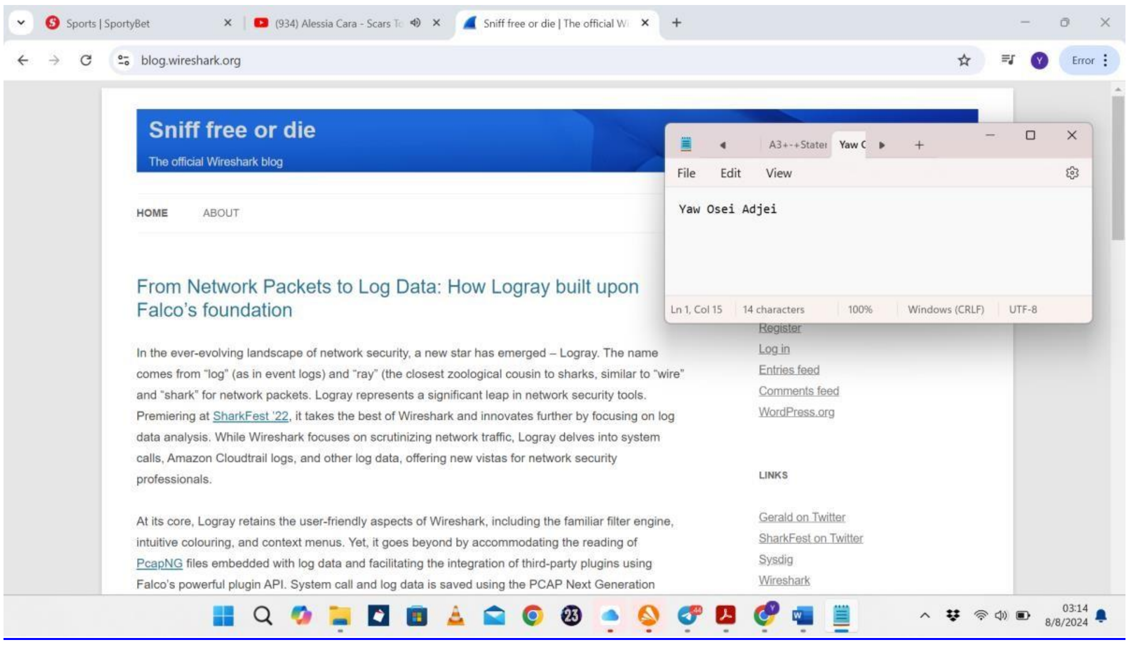
Readme
Apache-2.0 license
Activity
9.4k stars
152 watching
1.2k forks
Report repository

03:13
8/8/2024

Fig 1.9

3. Wireshark: A network protocol analyzer used to capture and analyze network traffic.

   Link: https://www.wireshark.org/



Sniff free or die

The official Wireshark blog

Yaw Osei Adjei

From Network Packets to Log Data: How Logray built upon Falco's foundation

In the ever-evolving landscape of network security, a new star has emerged – Logray. The name comes from "log" (as in event logs) and "ray" (the closest zoological cousin to sharks, similar to "wire" and "shark" for network packets. Logray represents a significant leap in network security tools. Premiering at SharkFest '22, it takes the best of Wireshark and innovates further by focusing on log data analysis. While Wireshark focuses on scrutinizing network traffic, Logray delves into system calls, Amazon Cloudtrail logs, and other log data, offering new vistas for network security professionals.

At its core, Logray retains the user-friendly aspects of Wireshark, including the familiar filter engine, intuitive colouring, and context menus. Yet, it goes beyond by accommodating the reading of PcapNG files embedded with log data and facilitating the integration of third-party plugins using Falco's powerful plugin API. System call and log data is saved using the PCAP Next Generation

Register
Log in
Entries feed
Comments feed
WordPress.org

LINKS

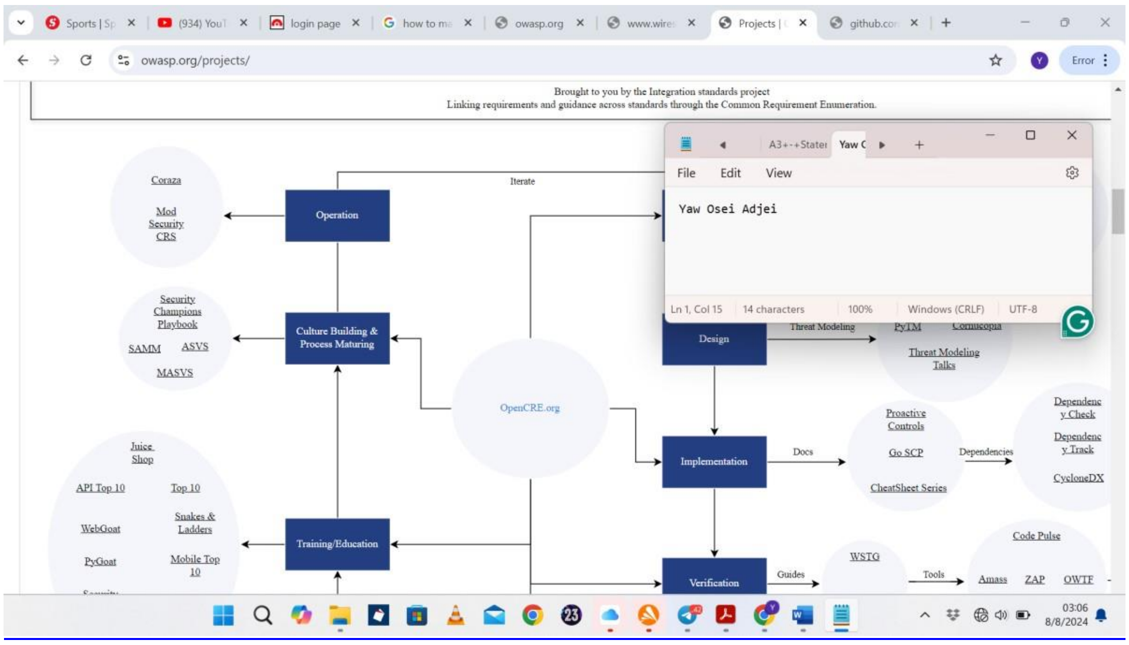
Gerald on Twitter
SharkFest on Twitter
Sysdig
Wireshark

03:14
8/8/2024

Fig 2.0

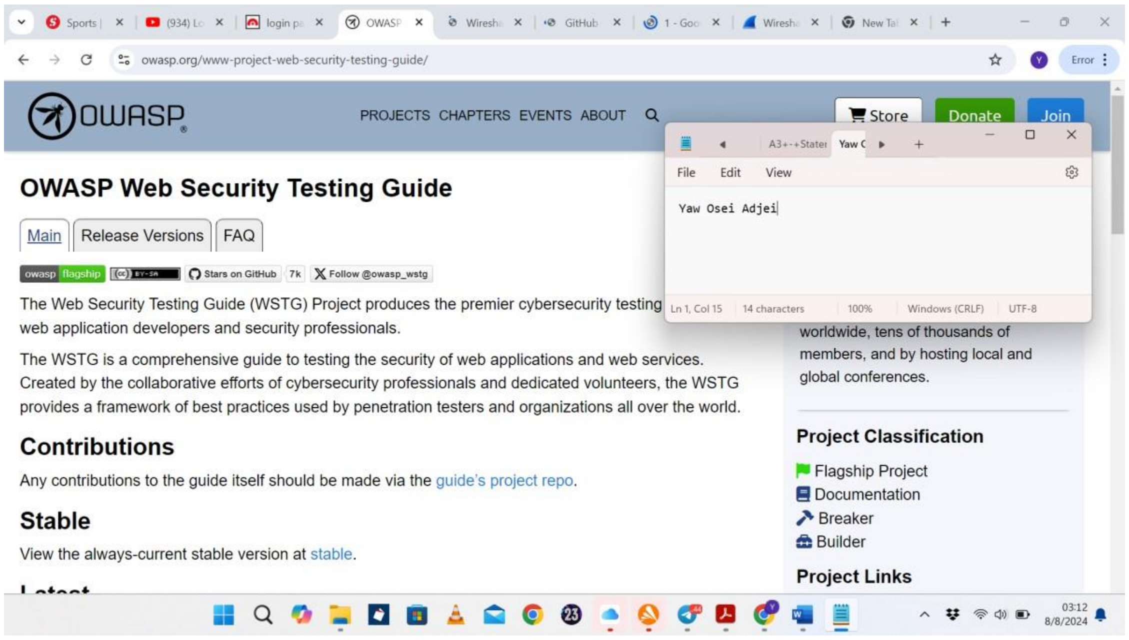
4. Wordlists: Lists of common directory names used for brute forcing directories.

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



[Fig](#) 2.1

6. Educational Materials: Tutorials and guides on web security testing techniques. Examples: https://owasp.org/www-project-web-security-testing-guide/ , various cybersecurity blogs and forums.


owasp.org/www-project-web-security-testing-guide/
PROJECTS CHAPTERS EVENTS ABOUT
Store
Donate
Join
Yaw Osei Adjei
Main
Release Versions
FAQ

OWASP Web Security Testing Guide

The Web Security Testing Guide (WSTG) Project produces the premier cybersecurity testing web application developers and security professionals.

The WSTG is a comprehensive guide to testing the security of web applications and web services. Created by the collaborative efforts of cybersecurity professionals and dedicated volunteers, the WSTG provides a framework of best practices used by penetration testers and organizations all over the world.

Contributions

Any contributions to the guide itself should be made via the guide's project repo.

Stable

View the always-current stable version at stable.

worldwide, tens of thousands of members, and by hosting local and global conferences.

Project Classification

Flagship Project
Documentation
Breaker
Builder

Project Links

Fig 2.2