UNIVERSITÀ DEGLI STUDI DI SALERNO

CORSO DI PENETRATION TESTING AND ETHICAL HACKING

Penetration Testing Report

Toppo: 1

ANNO ACCADEMICO
2024-2025

STUDENTE
Catello Staiano
Matricola: 0522501602

04/11/2025

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Indice

CAPITOLO 1

Penetration Testing Report

1.1 Executive Summary

Per l'espletamento della disciplina *Penetration Testing and Ethical Hacking*, è stata condotta un'analisi su un ambiente virtuale compromettibile, denominato `Toppo:1`, reperibile all'indirizzo `https://www.vulnhub.com/entry/toppo-1,245/`. L'obiettivo primario di tali operazioni è stato esclusivamente a scopo didattico, finalizzato a consolidare le nozioni teoriche impartite nel corso della disciplina. L'indagine è stata realizzata adottando una metodologia di approccio *Black-Box*, senza quindi disporre di alcuna informazione preliminare sull'infrastruttura bersaglio, e si è svolta all'interno di un contesto isolato con interconnessione diretta all'asset. Nel corso delle diverse attività svolte, sono state identificate molteplici debolezze di sicurezza che potrebbero consentire a un attore malevolo di ottenere l'accesso a dati e risorse riservate. Nel caso più grave, tali vulnerabilità potrebbero portare a una compromissione completa dell'integrità del sistema.

1.2 Engagement Highlights

La presente attività di *penetration testing* è stata concepita con finalità esclusivamente didattiche. Pertanto, non è stato stipulato alcun accordo contrattuale con un cliente. Per la fase di ricognizione e l'esecuzione delle operazioni, sono stati impiegati gli strumenti più efficaci, senza particolari vincoli. L'intero progetto ha rispettato la metodologia e le fasi acquisite durante il corso, articolandosi come segue:

1. *Information Gathering & Target Discovery*;
2. *Enumerating Target & Port Scanning*;
3. *Vulnerability Mapping*;
4. *Target Exploitation*;
5. *Post-Exploitation (privilege escalation)*;
6. *Post-Exploitation (maintaining access)*.

Gli strumenti utilizzati includono:

- `Netdiscover`
- `Nmap`
- `Gobuster`
- `Nessus`
- `OWASP ZAP`
- `Nikto`
- `Metasploit`
- `Msfvenom`
- `Dirb`
- `Whatweb`
- `Wafw00f`

1.3 Vulnerability Report

Nel corso della verifica di sicurezza sul sistema bersaglio, sono state riscontrate diverse lacune di sicurezza. Di seguito è riportata una rassegna dei principali punti deboli rilevati, categorizzati in base alla loro criticità:

- **Severity: Critica** `Debian Linux SEoL (8.x)`: Il sistema operativo identificato è Debian Linux 8.x (Jessie), una versione ormai fuori supporto (End of Life). Quindi il sistema può contenere vulnerabilità non risolte che possono essere sfruttate da attaccanti per ottenere accesso non autorizzato, eseguire codice arbitrario o compromettere la stabilità del sistema.

- **Severity: Media** `Vulnerabilità in versioni obsolete di JQuery`: La presenza di `JQuery` 1.2 < 3.5.0 rende il sistema suscettibile a vulnerabilità di tipo *Multiple XSS* (Cross-Site Scripting), che possono consentire a un attaccante di iniettare codice malevolo nel browser degli utenti.

- **Severity: Media** `SSH Terrapin Prefix Truncation Weakness`: Questa vulnerabilità potrebbe compromettere l'integrità delle connessioni `SSH`, alterando i dati trasmessi.

- **Severity: Media**

  `Web Application Potentially Vulnerable to Clickjacking`: È stato rilevato che il server web non imposta gli header di sicurezza X-Frame-Options o Content-Security-Policy nelle risposte HTTP. L'assenza di tali header può rendere l'applicazione vulnerabile ad attacchi di tipo Clickjacking, nei quali un attaccante può indurre un utente a cliccare su elementi della pagina diversa da quelli che percepisce visivamente. Questo può comportare l'esecuzione involontaria di azioni fraudolente o indesiderate, come la modifica di impostazioni, la conferma di transazioni o la divulgazione di dati sensibili.

- **Severity: Media** `Browsable Web Directories`: Durante l'analisi è stato rilevato che più directory sul server web risultano esplorabili ("directory listing" attivo). Questo significa che un utente può visualizzare l'elenco dei file e delle sottodirectory presenti in determinate cartelle del server, senza la necessità di

autenticazione. Questa configurazione può potenzialmente esporre informazioni sensibili (come file di backup, script, configurazioni o credenziali), favorendo ulteriori attività di ricognizione o attacco.

- **Severity: Media** `Content Security Policy (CSP) Header Not Set`: Questa vulnerabilità si verifica quando un'applicazione web non imposta l'header HTTP Content-Security-Policy nella risposta del server. Quando l'header CSP non è presente, il browser non ha alcuna restrizione su quali risorse esterne possono essere caricate o eseguite. Questo lascia l'applicazione esposta a potenziali attacchi XSS e al caricamento di contenuti malevoli.

- **Severity: Media** `Vulnerable JS Library`: Questa vulnerabilità si verifica quando un'applicazione web utilizza una libreria JavaScript con versioni obsolete per avere falle di sicurezza sfruttabili da un attaccante per compromettere il sito o i suoi utenti.

- **Severity: Media** `OpenSSH User Enumeration Weakness`: consente a un aggressore remoto di accertare quali nomi utente esistono su un server OpenSSH rilevando risposte differenti in caso di autenticazione non riuscita, agevolando così attacchi di forza bruta o tecniche di ingegneria sociale.

- **Severity: Bassa** `ICMP Timestamp Request Remote Date Disclosure`: Questa debolezza può esporre informazioni relative alla data e all'ora di un sistema remoto, fornendo potenzialmente dati utili per le attività di ricognizione di un attaccante.

Ulteriori debolezze di entità minore ma significative includono:

- `Mancanza dell'header X-Content-Type-Options`: potrebbe portare ad attacchi di *MIME Confusion*.

- `Server Leaks Version Information via "Server" HTTP Response Header Field`: l'esposizione dei dettagli sulla versione del server può agevolare un aggressore nell'identificazione di ulteriori vulnerabilità note relative a quella specifica versione.

- `OpenSSH Detection`: un server SSH esposto potrebbe costituire un vettore di attacco se configurato in modo non sicuro (es. accesso root abilitato, password deboli, chiavi non protette).

1.4 Remediation Report

Nel corso dell'analisi svolta, sono state individuate molteplici lacune di sicurezza rilevanti che potrebbero condurre a una compromissione totale del sistema, dei dati in esso contenuti e delle informazioni sensibili dei visitatori del sito web. Per tale ragione, si forniscono le seguenti raccomandazioni per il rafforzamento della sicurezza dell'asset:

- **Sistema operativo non più supportato: `Debian Linux 8.x (Jessie)`**

  Raccomandazioni: Aggiornare il sistema operativo a una versione di Debian attualmente supportata. Le versioni non più supportate non ricevono aggiornamenti di sicurezza né patch correttive, esponendo il sistema a vulnerabilità note e nuove.

  - **Azione**: Aggiornare il sistema operativo a una versione di Debian attualmente supportata (ad esempio `Debian 11 Bullseye` o `Debian 12 Bookworm`).

- **Vulnerabilità in librerie obsolete: `JQuery` < 3.5.0**

  Raccomandazioni: Utilizzare una versione aggiornata di `JQuery` superiore alla 3.5.0 per mitigare il rischio di attacchi di tipo *Cross-Site Scripting* (XSS). Le versioni datate rendono il sistema suscettibile a vulnerabilità critiche.

  - Azione: scaricare e implementare l'ultima versione da una rete di distribuzione contenuti (CDN) affidabile o dai repository ufficiali.

- **Mitigazione della debolezza `SSH` *Terrapin Prefix Truncation***

  Raccomandazioni: aggiornare il server `SSH` per sanare la vulnerabilità di troncamento del prefisso che può danneggiare l'integrità delle comunicazioni.

  - Azione: applicare le patch e gli aggiornamenti di sicurezza rilasciati dai fornitori del software `SSH`.

- **Prevenzione del *Clickjacking***

  Raccomandazioni: configurare l'header HTTP `X-Frame-Options` per impedire attacchi di *clickjacking*, circoscrivendo la visualizzazione del contenuto del sito al solo dominio di appartenenza.

  - Azione: aggiungere l'header `X-Frame-Options: DENY` o `X-Frame-Options: SAMEORIGIN` nei file di configurazione del server.

- **Disabilitazione del *Directory Browsing***

  Raccomandazioni: la navigazione delle directory rende accessibili i file e le cartelle del server, permettendo a un attaccante di ottenere informazioni riservate.

  - Azione: disabilitare l'accesso alle directory non necessarie nella configurazione del server web, ad esempio inserendo `Options -Indexes` nei file di configurazione di Apache.

- **Header di sicurezza non configurato: `Content-Security-Policy (CSP) Header Not Set`**

  Raccomandazioni: Configurare l'header `Content-Security-Policy` nelle risposte HTTP per limitare le sorgenti di contenuti che il browser può caricare ed eseguire. L'assenza di questa policy aumenta il rischio di attacchi di tipo *Cross-Site Scripting* (XSS) e di iniezione di contenuti malevoli.

  - **Azione**: Configurare l'intestazione CSP per limitare le fonti di contenuti approvati, ridu- cendo significativamente la superficie di attacco.

- **Aggiornamento delle librerie JavaScript vulnerabili**

  Raccomandazioni: sostituire o aggiornare le librerie JavaScript datate o compromesse presenti sul sito web.

  - Azione: eseguire una scansione completa delle dipendenze del progetto per assicurare che tutte le librerie siano aggiornate.

- **Configurazione dell'header `X-Content-Type-Options`**

  Raccomandazioni: aggiungere l'header `X-Content-Type-Options` con il valore `nosniff` per ostacolare attacchi basati sulla confusione del tipo MIME, che potrebbero indurre il browser a interpretare i file in modo errato.

  – Azione: modificare la configurazione del server web per includere `X-Content-Type-nosniff`.

- **Eliminazione di informazioni di debug e commenti superflui** *Raccomandazioni*: rimuovere commenti ambigui o informazioni di debug dalle pagine web che potrebbero fornire dettagli preziosi per gli aggressori.

  – Azione: eseguire una revisione del codice sorgente per eliminare commenti o informazioni riservate lasciate per errore.

- **Limitazione dell'esposizione delle informazioni di versione**

  Raccomandazioni: impedire che il server web riveli la versione del software in uso, poiché tali informazioni possono facilitare attacchi mirati.

  – Azione: configurare il server per non includere dettagli sulla versione negli header delle risposte (es. tramite la direttiva `ServerTokens Prod` per Apache).

1.5 Findings Summary

Le debolezze di sicurezza riscontrate nel corso della valutazione di penetrazione sono state ordinate in base al loro potenziale effetto sull'integrità del sistema. A tal fine, si presenta la seguente categorizzazione per criticità delle vulnerabilità:

- **Alta:** Punti deboli la cui sfruttabilità richiede prerequisiti specifici, ma che, una volta sfruttati, esercitano un impatto grave sul sistema. ($CVSS^3 \geq 7.5$)

- **Media:** Vulnerabilità la cui compromissione non è semplice da attuare, ma che, se sfruttate, possono causare un impatto considerevole. ($6.5 \leq CVSS^3 < 7.5$)

- **Bassa:** Debolezze che possiedono un impatto trascurabile e una bassa probabilità di essere sfruttate, e pertanto, non costituiscono una minaccia immediata di rilievo per il sistema. ($4.5 \leq CVSS^3 < 6.5$)
- **Informativa:** Non si tratta di vulnerabilità attuali, bensì di elementi informativi su configurazioni che in futuro potrebbero degenerare in vulnerabilità. ($CVSS^3 < 4$)

La tabella che segue riassume il numero di vulnerabilità rilevate per ciascuna categoria, facendo riferimento al solo host individuato, ovvero la macchina `Toppo`.

Host	Indirizzo IP	Alta	Media	Bassa	Informativa
`TOPPO: 1`	`10.0.2.5`	1	4	1	45

Tabella 1.1: Classificazione delle vulnerabilità

Di seguito vengono presentati un diagramma circolare per una valutazione più minuziosa della ripartizione delle vulnerabilità, e un grafico a colonne per illustrarne il computo totale.

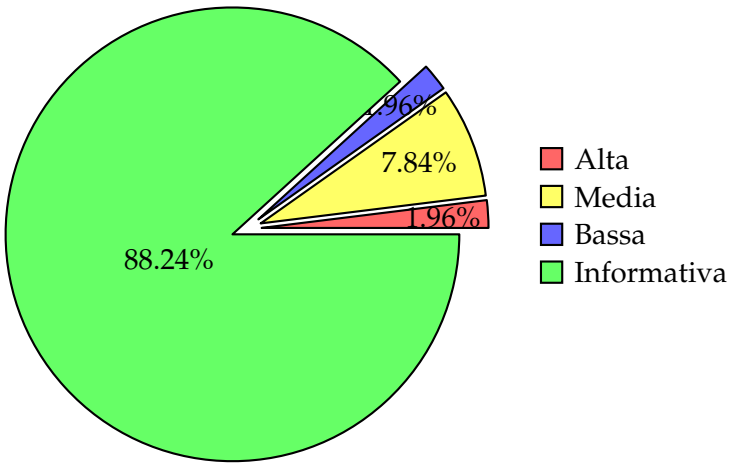

Figura 1.1: Diagramma circolare delle vulnerabilità

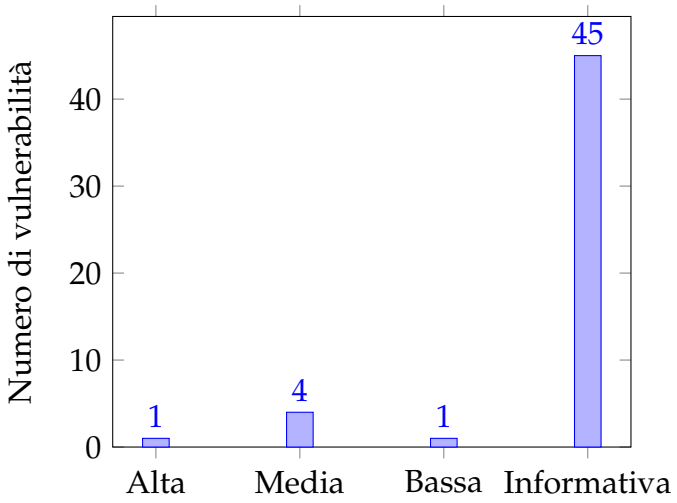

Figura 1.2: Grafico a colonne della distribuzione delle vulnerabilità

1.6 Detailed Summary

La seguente sezione illustra e analizza in dettaglio le lacune di sicurezza individuate tramite i diversi strumenti di scansione.

Debian Linux SEoL (8.x)	
CVE	
Rischio	ALTO
Descrizione	Il sistema operativo in uso è una versione ormai fuori supporto. Il fornitore (Debian Project) ha cessato il rilascio di aggiornamenti di sicurezza, correzioni di bug e patch per vulnerabilità note. Di conseguenza, il sistema può contenere vulnerabilità non risolte che possono essere sfruttate da attaccanti per ottenere accesso non autorizzato, eseguire codice arbitrario o compromettere la stabilità del sistema.
Impatto	L'assenza di aggiornamenti di sicurezza espone il sistema a possibili compromissioni totali, escalation di privilegi, o interruzione dei servizi. Eventuali vulnerabilità note nelle componenti di sistema o nei pacchetti installati non verranno corrette, aumentando il rischio di attacchi mirati.
Soluzione	Aggiornare il sistema operativo a una versione di Debian attualmente supportata dal fornitore (ad esempio Debian 11 "Bullseye" o Debian 12 "Bookworm"). Dopo l'aggiornamento, eseguire una nuova scansione di sicurezza per verificare la rimozione della vulnerabilità e la presenza di eventuali nuovi problemi introdotti dal processo di upgrade.
Metodo di detection	La vulnerabilità è stata rilevata con l'ausilio del software `Nessus`.

JQuery 1.2 < 3.5.0 Multiple XSS	
CVE	2020-11022/11023
Rischio	MEDIO
Descrizione	La versione della libreria JQuery in uso sul server web presenta diverse lacune di sicurezza che la rendono soggetta a numerosi punti debolezza di tipo cross-site scripting (XSS).
Impatto	Un aggressore ha la possibilità di avvalersi di tali debolezze per iniettare ed eseguire codice malevolo all'interno dell'ambiente di sicurezza del browser del bersaglio.
Soluzione	Installare una versione di JQuery 3.5.0 o più recente.
Metodo di detection	La vulnerabilità è stata rilevata con l'ausilio del software Nessus.

SSH Terrapin Prefix Truncation Weakness	
CVE	2023-48795
Rischio	MEDIO
Descrizione	Un server SSH esterno risulta suscettibile a un'aggressione di tipo "man-in-the-middle" che sfrutta il troncamento del prefisso, consentendo a un aggressore di eludere le verifiche di integrità e compromettere l'affidabilità della connessione.
Impatto	Un aggressore può abusare di questa debolezza per intercettare o alterare il contenuto della connessione SSH.
Soluzione	Aggiornare il server SSH e adottare protocolli di sicurezza più affidabili.
Metodo di detection	La vulnerabilità è stata rilevata con l'ausilio del software Nessus.

Web Application Potentially Vulnerable to Clickjacking	
CVE	
Rischio	MEDIO
Descrizione	Il sistema remoto presenta una o più condivisioni Windows accessibili in rete con le credenziali fornite. A seconda delle autorizzazioni di condivisione, un aggressore potrebbe essere in grado di leggere o scrivere dati confidenziali.
Impatto	A causa di questa vulnerabilità, gli utenti possono essere ingannati e indotti a selezionare elementi non visibili, i quali eseguono azioni dannose senza che se ne rendano conto. Tale attività può portare a violazioni di sicurezza significative, come la fuoriuscita di dati sensibili o l'esecuzione di comandi non autorizzati.
Soluzione	I moderni browser web sono in grado di supportare le intestazioni HTTP Content-Security-Policy e X-Frame-Options. Assicurati che una di queste sia configurata su ogni pagina web restituita dal tuo sito o dalla tua applicazione. Se prevedi che la pagina venga visualizzata in un frame solo da pagine che fanno parte dello stesso sito (ad esempio, un FRAMESET), puoi usare SAMEORIGIN. Altrimenti, se non vuoi che la pagina non sia mai inserita in un frame, dovresti usare DENY. In alternativa, considera di implementare la direttiva frame-ancestors della Content Security Policy.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus` ma anche con l'ausilio dei software `OWASP ZAP` e `Nikto` con il nome di *Missing Anti-clickjacking Header*.

Browsable Web Directories	
CVE	
Rischio	MEDIO
Descrizione	La navigazione degli indici di directory è abilitata. Questa esposizione potrebbe rivelare file di script nascosti, file di inclusione, file di backup e altri dati sensibili, rendendoli leggibili a utenti non autorizzati.
Impatto	Gli aggressori possono acquisire informazioni sui file e sulle directory, semplificando così attacchi futuri diretti verso il sistema.
Soluzione	Disattivare la navigazione degli indici di directory all'interno del file di configurazione del server web.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio dei software `Nessus` ma anche con i software `OWASP ZAP` e `Nikto` con il nome di *Directory Browsing*.

Content Security Policy (CSP) Header Not Set	
CVE	`2018-5164`
Rischio	MEDIO
Descrizione	L'intestazione HTTP Content Security Policy (CSP) non è impostata. La CSP rappresenta una difesa efficace contro varie tipologie di attacchi, come l'XSS (Cross-Site Scripting).
Impatto	L'assenza della Content Security Policy (CSP) consente l'iniezione di codice maligno nel contesto dell'utente, incrementando il rischio di attacchi XSS e di altre minacce informatiche.
Soluzione	Configurare l'intestazione CSP per circoscrivere le fonti di contenuti permessi, riducendo sensibilmente le possibili vie di attacco.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `OWASP ZAP`.

Vulnerable JS Library	
CVE	`2020-11023/11022/829`
Rischio	MEDIO
Descrizione	Un sito web impiega una libreria JavaScript obsoleta, che può consentire l'esecuzione di codice dannoso o l'esposizione di dati riservati.
Impatto	Un aggressore può abusare di queste debolezze per iniettare codice maligno nel contesto del browser della vittima, compromettendo la sicurezza delle sessioni e ottenendo l'accesso a dati riservati.
Soluzione	Aggiornare tutte le librerie JavaScript vulnerabili alla versione più recente e assicurarsi che vengano mantenute e aggiornate regolarmente.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `OWASP ZAP`.

OpenSSH User Enumeration Weakness	
CVE	2018-15473
Rischio	MEDIO
Descrizione	Un host che esegue il software OpenSSH è suscettibile a una vulnerabilità di enumerazione degli account, la quale permette a un aggressore di accertare l'esistenza di specifici nomi utente su un sistema di destinazione. Questa debolezza si manifesta attraverso le diverse risposte fornite dal server durante i tentativi di autenticazione, a seconda che il nome utente sia valido o meno. Tale esposizione può favorire attacchi successivi, come brute-force o tattiche di ingegneria sociale.
Impatto	Un aggressore può avvalersi di questa debolezza per determinare quali account utente esistono sul sistema remoto. Ciò semplifica la creazione di un elenco di nomi utente validi per futuri attacchi mirati come il brute-force o l'ingegneria sociale.
Soluzione	Aggiornare il server OpenSSH alla sua versione più recente, la quale integra le correzioni per impedire l'enumerazione degli utenti. Inoltre, è necessario configurare OpenSSH in modo che la risposta del server sia uniforme, indipendentemente dalla validità del nome utente fornito.
Metodo di detection	

ICMP Timestamp Request Remote Date Disclosure	
CVE	
Rischio	BASSO
Descrizione	Gli attaccanti possono abusare di queste informazioni per acquisire una conoscenza più dettagliata della struttura dell'applicazione e lanciare così attacchi mirati, come SQL injection o path traversal.
Impatto	Un aggressore può sfruttare le informazioni di timestamp per sferrare attacchi basati sulla tempistica.
Soluzione	È necessario impedire al sistema di rispondere alle richieste ICMP Timestamp.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

X-Content-Type-Options Header Missing	
CVE	`2019-19089`
Rischio	BASSO
Descrizione	L'intestazione X-Content-Type-Options non è impostata correttamente su 'nosniff', il che permette a browser datati di effettuare il MIME-sniffing sul corpo della risposta.
Impatto	Questa vulnerabilità può agevolare attacchi che si basano su un'erronea interpretazione del tipo di contenuto.
Soluzione	È necessario configurare le risposte HTTP in modo che includano l'intestazione X-Content-Type-Options impostata su 'nosniff'.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio dei software `OWASP ZAP` e `Nikto`.

Server Leaks Version Information via "Server" HTTP Response Header Field	
CVE	
Rischio	BASSO
Descrizione	Il server web o l'applicazione espone dettagli sulla propria versione attraverso l'header della risposta HTTP "Server". La disponibilità di queste informazioni può agevolare un aggressore nell'identificazione di ulteriori vulnerabilità che affliggono il server o l'applicazione stessa.
Impatto	L'esposizione dei dettagli sulla versione del server può agevolare la fase di ricognizione di un aggressore, consentendogli di mirare a vulnerabilità note relative a quella specifica versione.
Soluzione	È necessario configurare il server web per evitare che divulghi informazioni sulla sua versione all'interno dell'header di risposta Server. Tale misura può essere attuata modificando le impostazioni del server o impiegando appositi moduli di sicurezza.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `OWASP ZAP`.

Content-Type Header Missing	
CVE	
Rischio	INFORMATIVO
Descrizione	È stato rilevato che alcune risposte HTTP del server non includono l'header "Content-Type". Questo header è fondamentale per indicare al browser o al client quale tipo di contenuto viene restituito. In assenza di tale informazione, il browser può tentare di determinare autonomamente il tipo MIME del contenuto ("MIME sniffing").
Impatto	L'assenza dell'header "Content-Type" può indurre il browser a interpretare erroneamente il contenuto, favorire attacchi XSS (Cross-Site Scripting) o code injection, causare problemi di visualizzazione o comunicazione errata tra client e server.
Soluzione	Configurare il server o l'applicazione affinché tutte le risposte HTTP includano un header "Content-Type" corretto e coerente con il contenuto restituito.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio dei software `OWASP ZAP` e `Nikto`.

Information Disclosure - Suspicious comment	
CVE	
Rischio	INFORMATIVO
Descrizione	È stata individuata la presenza di commenti sospetti o informativi all'interno del codice sorgente HTML o di file JavaScript accessibili pubblicamente. Questi commenti possono contenere informazioni sensibili che possono essere utilizzate da un attaccante per ottenere una migliore comprensione della struttura interna dell'applicazione o pianificare ulteriori attacchi.
Impatto	La divulgazione involontaria di informazioni interne può facilitare attacchi mirati, esporre dati sensibili come credenziali, chiavi API, o percorsi di file di sistema, rivelare dettagli sull'architettura o logica di business dell'applicazione. In combinazione con altre vulnerabilità, può aumentare significativamente la superficie d'attacco dell'applicazione.
Soluzione	Rimuovere tutti i commenti sensibili o informativi dal codice sorgente prima della pubblicazione in ambiente di produzione, effettuare una revisione del codice per assicurarsi che non siano presenti riferimenti a funzioni di debug, credenziali o percorsi interni, e implementare un processo di code review o un controllo automatizzato per intercettare eventuali informazioni non sicure nei file pubblici.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `OWASP ZAP`.

Modern Web Application	
CVE	`N/A`
Rischio	INFORMATIVO
Descrizione	È stato riscontrato che l'applicazione web moderna presenta diverse problematiche di sicurezza. Sono state identificate configurazioni errate e mancanza di controlli robusti lato server, potenzialmente esponendo l'applicazione ad attacchi di tipo Cross-Site Scripting (XSS), Insecure Direct Object Reference (IDOR), Cross-Site Request Forgery (CSRF) e data exposure.
Impatto	Le vulnerabilità identificate possono consentire a un attaccante di accedere a dati sensibili, impersonare altri utenti, manipolare richieste o compromettere l'integrità dell'applicazione. L'assenza di protezioni adeguate a livello di autenticazione e validazione input può compromettere la riservatezza dei dati degli utenti e violare requisiti di conformità.
Soluzione	Implementare una validazione e sanificazione robusta degli input utente sia lato client che lato server, assicurare controlli di accesso granulari per ogni endpoint, abilitare le intestazioni di sicurezza HTTP e configurare correttamente CORS. Applicare rate limiting sugli endpoint sensibili e aggiornare tutte le dipendenze di terze parti tramite un sistema di gestione vulnerabilità.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `OWASP ZAP`.

User Agent Fuzzer	
CVE	`N/A`
Rischio	INFORMATIVO
Descrizione	È stato rilevato che lo strumento "User Agent Fuzzer", utilizzato per testare la robustezza dei server HTTP, non implementa adeguate misure di sanitizzazione e isolamento dei payload generati. Le stringhe User-Agent malevoli o eccessivamente lunghe possono causare problemi di stabilità, manipolazione dei log o potenziali command injection se passate a comandi di sistema senza escaping.
Impatto	Un uso improprio o non isolato del fuzzer può comportare l'esecuzione di comandi arbitrari sul sistema che lo ospita (RCE), corruzione dei log tramite log forging o denial of service per esaurimento delle risorse. Inoltre, l'esecuzione non controllata su target esterni può costituire una violazione legale.
Soluzione	Validare e filtrare tutte le stringhe User-Agent prima dell'uso, evitando l'interpolazione diretta in comandi shell. Implementare limiti di lunghezza e timeout per prevenire DoS, usare formati di log strutturati (es. JSON), ed eseguire il fuzzer in ambienti isolati. Aggiungere una modalità "safe" che escluda payload distruttivi e inserire un avviso legale all'avvio per l'utilizzo etico dello strumento.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `OWASP ZAP`.

Apache Banner Linux Distribution Disclosure	
CVE	
Rischio	INFORMATIVO
Descrizione	Le informazioni sulla distribuzione Linux, divulgate dal banner di Apache, possono essere utilizzate da un attaccante per individuare falle di sicurezza note e mirate a quella specifica versione del sistema operativo.
Impatto	L'esposizione dei dettagli sulla distribuzione Linux in uso può agevolare la fase di ricognizione di un aggressore, consentendogli di prendere di mira vulnerabilità specifiche di quella distribuzione.
Soluzione	È necessario modificare le impostazioni di Apache per impedire la visualizzazione delle informazioni sulla distribuzione all'interno del suo banner.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

Apache HTTP Server Version	
CVE	
Rischio	INFORMATIVO
Descrizione	Il server Apache HTTP su questo sistema rivela la versione in uso. Questa informazione può essere utilizzata da un aggressore per identificare potenziali vulnerabilità specifiche della versione.
Impatto	L'esposizione dei dettagli sulla versione del server Apache HTTP può agevolare la fase di ricognizione di un aggressore, consentendogli di prendere di mira vulnerabilità specifiche note per quella versione.
Soluzione	Configurare il server web per nascondere i dettagli sulla versione di Apache HTTP dal suo banner.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

Backported Security Patch Detection (WWW)	
CVE	
Rischio	INFORMATIVO
Descrizione	È stata riscontrata la presenza di patch di sicurezza backportate per il server web. Queste patch includono correzioni per vulnerabilità ma non alterano il numero di versione del software, il che rende più complessa la verifica manuale della loro applicazione.
Impatto	Le patch di sicurezza backportate consentono di mantenere il sistema protetto senza la necessità di eseguire aggiornamenti completi del software. Tuttavia, la mancata corrispondenza del numero di versione può confondere gli strumenti di sicurezza automatizzati.
Soluzione	Per proteggersi dalle vulnerabilità conosciute, è necessario controllare con regolarità la disponibilità di aggiornamenti di sicurezza e installarli senza ritardo.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

Common Platform Enumeration (CPE)	
CVE	
Rischio	INFORMATIVO
Descrizione	Questo strumento rileva e registra le informazioni CPE (Common Platform Enumeration) associate ai software e ai sistemi che sono stati individuati nel corso della scansione.
Impatto	L'adozione degli standard CPE facilita una gestione più accurata delle risorse IT e delle vulnerabilità ad esse correlate.
Soluzione	Sfruttare i dati CPE per una valutazione e una gestione efficaci delle vulnerabilità, garantendo l'installazione di tutte le correzioni di sicurezza pertinenti.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

Device Type	
CVE	
Rischio	INFORMATIVO
Descrizione	Basandosi sui dati raccolti, questo strumento è in grado di determinare la categoria di ogni dispositivo rilevato, ad esempio se si tratta di un router, uno switch o un server.
Impatto	Conoscere il tipo di apparato permette di sviluppare attacchi specifici o, in un contesto difensivo, di ottimizzare la gestione delle risorse di rete.
Soluzione	Sfrutta i dati sul tipo di dispositivo per una gestione più efficace della sicurezza e per garantire che tutti gli apparati siano configurati e protetti correttamente.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

Ethernet Card Manufacturer Detection	
CVE	
Rischio	INFORMATIVO
Descrizione	Questo strumento è in grado di riconoscere il fabbricante delle schede di rete Ethernet presenti su un sistema remoto.
Impatto	Conoscere il fabbricante delle schede di rete può agevolare la scoperta di vulnerabilità mirate e legate a quel preciso hardware.
Soluzione	Verificare che i driver e il firmware delle schede di rete siano installati con le più recenti correzioni di sicurezza.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

Ethernet MAC Addresses	
CVE	
Rischio	INFORMATIVO
Descrizione	Questo strumento è in grado di identificare gli indirizzi fisici (MAC) delle interfacce di rete di un sistema remoto.
Impatto	L'uso degli indirizzi MAC permette di riconoscere e tenere sotto controllo i dispositivi individuali presenti sulla rete.
Soluzione	Sfruttare le informazioni sugli indirizzi MAC per una gestione e un monitoraggio efficiente della rete, applicando le politiche di sicurezza appropriate.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

HTTP Server Type and Version	
CVE	
Rischio	INFORMATIVO
Descrizione	Questo strumento è in grado di determinare il tipo e la versione del web server installato su un sistema remoto.
Impatto	L'identificazione della tipologia e della versione del server HTTP può agevolare un aggressore nella pianificazione di attacchi mirati, in quanto gli consente di sfruttare vulnerabilità già note.
Soluzione	È fondamentale garantire che il server HTTP sia sempre aggiornato con le ultime patch di sicurezza e che la sua configurazione segua le migliori pratiche di sicurezza.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

HyperText Transfer Protocol (HTTP) Information	
CVE	
Rischio	INFORMATIVO
Descrizione	Durante la scansione, questo strumento acquisisce dati dai server web individuati, come header, cookie e diverse informazioni di configurazione.
Impatto	I dati acquisiti possono essere impiegati per individuare falle di sicurezza e per ottimizzare la configurazione del web server.
Soluzione	È consigliabile impiegare le informazioni raccolte per configurare il server HTTP in modo sicuro e per applicare tutte le patch di sicurezza necessarie.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

JQuery Detection	
CVE	
Rischio	INFORMATIVO
Descrizione	Questo strumento è in grado di rilevare la libreria jQuery su un host remoto e di utilizzare tale informazione per individuare potenziali vulnerabilità nella versione in esecuzione.
Impatto	L'identificazione dell'utilizzo di jQuery può agevolare un aggressore nella pianificazione di attacchi mirati, in quanto gli consente di sfruttare vulnerabilità note della libreria.
Soluzione	È fondamentale utilizzare l'ultima versione stabile di jQuery e mantenere aggiornate tutte le librerie, al fine di mitigare i rischi per la sicurezza.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

Nessus SYN scanner	
CVE	
Rischio	INFORMATIVO
Descrizione	Questo plugin è uno scanner di porte SYN 'half-open', relativamente veloce e capace di bypassare anche host protetti da firewall. Sebbene le scansioni SYN siano meno intrusive di quelle TCP complete, possono causare problemi ai firewall meno robusti e lasciare connessioni non chiuse sul sistema remoto in caso di elevato traffico di rete.
Impatto	Una scansione SYN può essere impiegata per individuare i servizi attivi su un host remoto. Questa informazione è utile per la pianificazione di ulteriori controlli di sicurezza o per la preparazione di attacchi mirati.
Soluzione	È necessario mettere in sicurezza il target utilizzando una politica di filtraggio degli indirizzi IP.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

Nessus Scan Information	
CVE	
Rischio	INFORMATIVO
Descrizione	Questo strumento raccoglie dati approfonditi sulle scansioni effettuate con Nessus, riportando informazioni complete su host, plugin e risultati.
Impatto	I risultati dell'analisi servono a valutare la sicurezza di un sistema e a definire le azioni correttive da intraprendere.
Soluzione	È consigliabile utilizzare le informazioni raccolte per migliorare la configurazione di sicurezza del sistema e per risolvere le vulnerabilità individuate.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

OS Identification	
CVE	
Rischio	INFORMATIVO
Descrizione	Questo strumento rileva il sistema operativo in esecuzione su un host remoto, un dato utile per individuare vulnerabilità specifiche di quel sistema.
Impatto	L'identificazione del sistema operativo può agevolare un aggressore nella pianificazione di attacchi mirati, in quanto gli consente di sfruttare le vulnerabilità note e specifiche di quella piattaforma.
Soluzione	È fondamentale garantire che il sistema operativo sia sempre aggiornato con le ultime patch di sicurezza e che sia configurato in conformità con le migliori pratiche del settore.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

Patch Report	
CVE	
Rischio	INFORMATIVO
Descrizione	Questo strumento produce un resoconto sullo stato delle patch, utile per verificare la rispondenza del sistema agli standard di sicurezza.
Impatto	L'identificazione del sistema operativo può agevolare un aggressore nella pianificazione di attacchi mirati, in quanto gli consente di sfruttare le vulnerabilità note e specifiche di quella piattaforma.
Soluzione	Installare le patch di sicurezza necessarie.
Metodo di detection	Questa falla di sicurezza è stata rilevata con l'ausilio del software `Nessus`.

CAPITOLO 2

Appendix

Una prova dello sfruttamento della vulnerabilità è descritta nel documento StaianoCatello_Metodologia, reperibile anche a questo link:

`https://github.com/staianocatello/Penetration_Testing_Toppo-1`

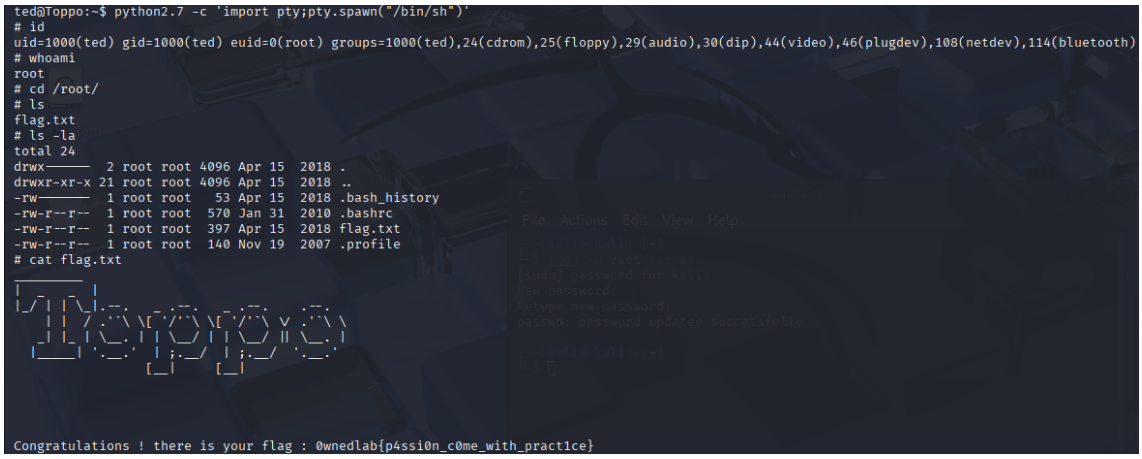

Figura 2.1: Bandiera catturata

Bibliografia

[1] CVE-2020-11022, *Cross-site scripting (XSS) vulnerability in jQuery*, NVD - National Vulnerability Database.

[2] CVE-2020-11023, *Cross-site scripting (XSS) vulnerability in jQuery*, NVD - National Vulnerability Database.

[3] CVE-2023-48795, NVD - National Vulnerability Database.

[4] CVE-2018-5164, *Out-of-bounds write vulnerability in Mozilla Firefox*, NVD - National Vulnerability Database.

[5] CVE-2020-0829, *Remote Code Execution vulnerability in Microsoft Office*, NVD - National Vulnerability Database.

[6] CVE-2018-15473, *User Enumeration Vulnerability in OpenSSH*, NVD - National Vulnerability Database.

[7] CVE-2019-19089, *Memory leak vulnerability in the Linux Kernel*, NVD - National Vulnerability Database.