Università degli Studi di Salerno

Penetration Testing Report

CASO DI STUDIO: **PHOTOGRAPHER 1**

Davide Di Sarno | Corso di PTEH | A.A. 2023/2024

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Sommario

Executive Summary

Per il progetto di Penetration Testing è stato scelto di effettuare un processo di penetration testing etico sulla macchina virtuale **PHOTOGRAPHER: 1**, reperibile sulla piattaforma VulnHub al seguente link:

https://www.vulnhub.com/entry/photographer-1,519/

Questa macchina consente agli utenti di esercitarsi per l'OSCP nell'enumerazione delle condivisioni SMB e dei servizi web, trovando suggerimenti per le password per accedere a un'applicazione web vulnerabile ed esercitandosi nell'RCE tramite caricamento di file arbitrari. Inoltre, offre l'opportunità di praticare l'escalation dei privilegi enumerando i binari SUID e utilizzandoli per ottenere privilegi a livello root.

Gli obiettivi da raggiungere sono i seguenti:
- Enumerare i servizi e le vulnerabilità presenti sulla macchina target;
- Prendere possesso della macchina target accedendo come root;
- Prendere possesso del flag *user.txt*;
- Prendere possesso del flag *proof.txt*;

L'attività di penetration testing sulla macchina target ha avuto inizio il 28/06/2024. Questo testing rientra nella categoria del grey box testing poiché avevamo conoscenza del sistema operativo presente sulla macchina target ma non avevamo informazioni cruciali come l'indirizzo IP e i servizi attivi.
Durante la fase di penetration testing, abbiamo seguito i principi di un hacker white-hat, con l'obiettivo di identificare e documentare eticamente le vulnerabilità del sistema, fornendo soluzioni per mitigare i problemi di sicurezza riscontrati.

Questo report illustrerà tutte le vulnerabilità che sono state individuate durante il processo di penetration testing. In particolare, le vulnerabilità rilevate possono permettere a un attaccante di ottenere il pieno controllo del sistema e assumere i privilegi di amministratore. È anche possibile che un attaccante rubi dati sensibili degli utenti del sito web.

Attualmente, il livello di rischio complessivo associato all'asset risulta essere critico. Tuttavia, mediante l'adozione di diverse misure, come la rimozione dei dati sensibili dalle risorse pubbliche e l'implementazione di controlli semplici, è possibile ridurre sensibilmente il livello di rischio.

Engagement Highlights

L’attività di penetration testing che verrà eseguita ha scopi didattici e, pertanto, non è stata stipulata alcuna contrattazione con un cliente. Saranno utilizzati gli strumenti più efficienti per la ricerca delle informazioni e l'esecuzione dei task, senza particolari limitazioni.
L’intero progetto ha seguito le fasi che sono state insegnate durante l’intero corso:
1. Information Gathering & Target Discovery;
2. Enumeration 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
- P0f
- Nping
- Unicornscan
- Smbclient
- Dirb
- Nessus
- OpenVAS
- OWASP ZAP
- Nikto
- WhatWeb
- Searchsploit
- Burp Suite
- Netcat
- Metasploit

Vulnerability Report

Nel corso del processo di Penetration Testing sono state rilevate diverse vulnerabilità sfruttabili per compromettere vari aspetti del sistema. Di seguito riportiamo le principali vulnerabilità riscontrate.

- **[Severity: Alta] Accesso non autorizzato ai file condivisi su Windows**:
  Le impostazioni di condivisione di file su Windows permettono a utenti non autorizzati di accedere a dati sensibili;

- **[Severity: Alta] Caricamento di file non autorizzati su Koken CMS**:
  Questa vulnerabilità consente ad un utente autenticato di caricare file non autorizzati sul server, eludendo le restrizioni sui tipi di file permessi;

- **[Severity: Media] Vulnerabilità in versioni obsolete di JQuery**:
  Utilizzare versioni obsolete di JQuery può consentire ad attaccanti di inserire codice malevolo nelle pagine web, compromettendo la sicurezza degli utenti;

- **[Severity: Media] Assenza di token di sicurezza nelle richieste web**:
  La mancanza di token di sicurezza nelle richieste permette l'esecuzione di azioni non autorizzate a nome degli utenti autenticati;

- **[Severity: Media] Accesso alle directory del server web tramite browser:**
  Possibilità di navigare le directory del *Web Server* mediante il *Web Browser* al fine di visualizzarne il contenuto;

- **[Severity: Media] Mancanza di protezione dei dati trasmessi**:
  La firma dei dati trasmessi non è obbligatoria, permettendo agli attaccanti di modificarli, compromettendo l'integrità delle informazioni;

- **[Severity: Bassa] Informazioni sulla versione del server visibili nelle risposte**:
  Il server web fornisce dettagli sulla versione nelle risposte HTTP, aiutando gli attaccanti a identificare possibili vulnerabilità.

Remediation Report

Per eliminare le vulnerabilità riscontrate nel sistema e ridurre i rischi associati, si consiglia di seguire le operazioni descritte di seguito:

- **Rafforzamento delle restrizioni di accesso e aggiornamento delle configurazioni di sicurezza per le condivisioni di file su Windows**:
  Implementare politiche di accesso rigorose per le condivisioni SMB e aggiornare le configurazioni di sicurezza per limitare l'accesso a utenti autorizzati;

- **Aggiornamento di Koken CMS all'ultima versione sicura e implementazione di controlli sui file caricabili**:
  Installare l'ultima versione di Koken CMS per correggere la vulnerabilità del caricamento arbitrario di file e implementare restrizioni sui tipi di file accettati per evitare il caricamento di file non autorizzati;

- **Aggiornamento di JQuery all'ultima versione disponibile**:
  Sostituire le versioni obsolete di JQuery con la versione più recente per prevenire potenziali attacchi;

- **Implementazione di token di sicurezza in tutte le richieste e moduli critici**:
  Aggiungere token di sicurezza a tutte le forme e richieste critiche per prevenire attacchi che sfruttano richieste indesiderate;

- **Disabilitazione della navigazione delle directory nel server web**:
  Riconfigurare il server web per impedire la visualizzazione dei contenuti delle directory tramite browser, migliorando così la sicurezza.

- **Abilitazione della firma obbligatoria per tutte le connessioni di dati SMB**:
  Configurare il server SMB per richiedere la firma dei dati trasmessi, migliorando l'integrità delle informazioni.

- **Configurazione del server per nascondere o personalizzare l'intestazione "Server" nelle risposte HTTP**:
  Modificare le impostazioni del server web per evitare di rivelare informazioni sulla versione, riducendo così il rischio di sfruttamento delle vulnerabilità specifiche della versione.

Findings Summary

Le vulnerabilità identificate durante il penetration testing sono state classificate in base al loro potenziale impatto sul sistema. Di seguito viene presentata la classificazione per gravità delle vulnerabilità:

- **Alta**: vulnerabilità che richiedono determinati requisiti per poter essere sfruttate e hanno un impatto grave sul sistema. ($CVSS^3$ >= 7.5)
- **Media**: vulnerabilità non semplici da sfruttare e che hanno un impatto relativamente grave sul sistema. (6.5 <= $CVSS^3$ < 7.5)
- **Bassa**: vulnerabilità che hanno un impatto poco significativo e che hanno una bassa probabilità di essere sfruttate e, pertanto, non rappresentano, nell'immediato, una minaccia rilevante per il sistema. (4.5 <= $CVSS^3$ < 6.5)
- **Informativa**: non sono vulnerabilità, ma informazioni su configurazioni di software che nel futuro potrebbero generare delle vulnerabilità. ($CVSS^3$ < 4)

La tabella seguente mostra il numero di vulnerabilità individuate per ciascuna categoria relative all'unico host individuato, ovvero la macchina PHOTOGRAPHER:1:

Host	Indirizzo IP	Alta	Media	Bassa	Informativa
PHOTOGRAPHER:1	172.16.62.148	2	6	4	42

Figura 1: Classificazione delle vulnerabilità

Di seguito sono mostrati un grafico a torta per avere una visione più dettagliata sulla distribuzione delle vulnerabilità presenti e un ortogramma per visualizzarne il conteggio.

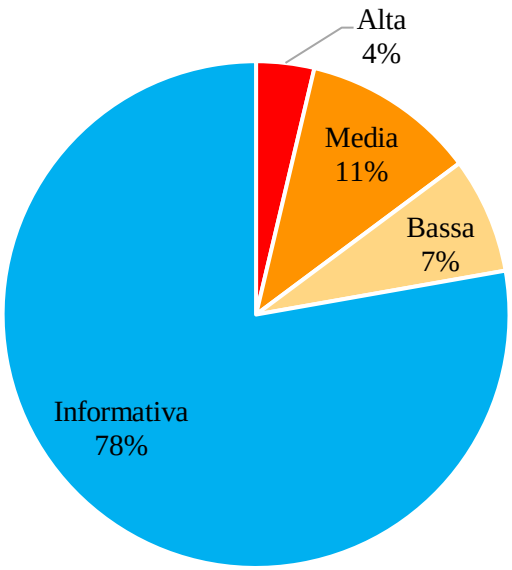

Figura 2: Aerogramma delle vulnerabilità riscontrate

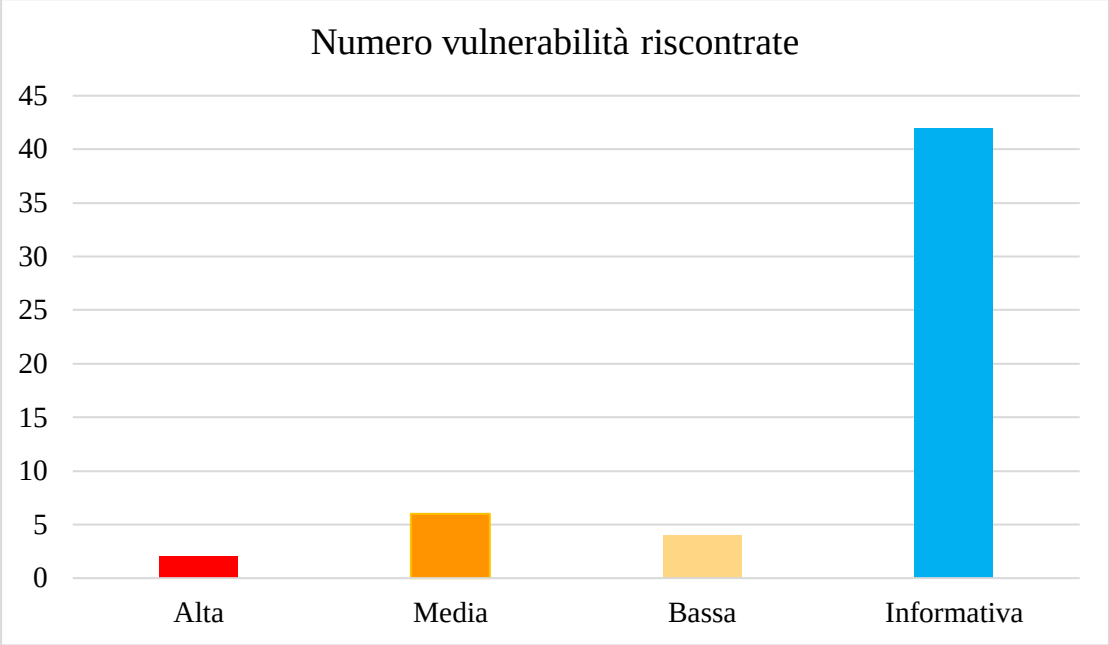

Figura 3: Istogramma delle vulnerabilità riscontrate

Detailed Summary

In questa sezione verranno elencate e descritte tutte le vulnerabilità riscontrate dai vari tool utilizzati.

Microsoft Windows SMB: Accesso non privilegiato alle condivisioni	CVE
	CVE-1999-0520
ALTA	
Descrizione: L'host remoto ha una o più condivisioni Windows a cui è possibile accedere tramite la rete con le credenziali fornite. A seconda dei diritti di condivisione, potrebbe consentire a un aggressore di leggere/scrivere dati riservati.	
Impatto: Questa vulnerabilità permette l'accesso non autorizzato alle condivisioni SMB di Windows, il che potrebbe portare a lettura e scrittura di dati sensibili. Un attaccante potrebbe sfruttare questa vulnerabilità per ottenere accesso non privilegiato ai file condivisi.	
Soluzione: Per restringere l'accesso, aprire Esplora risorse, fare clic con il tasto destro su ogni condivisione, andare alla scheda "Condivisione" e cliccare su "Permessi". Assicurarsi che solo gli utenti autorizzati abbiano accesso alle condivisioni.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Koken: Vulnerabilità nella versione 0.22.24	CVE
	-
ALTA	
Descrizione: La versione 0.22.24 di Koken presenta una vulnerabilità che potrebbe permettere a un attaccante di sfruttare specifiche debolezze nel sistema per compromettere l'integrità e la sicurezza dell'applicazione.	
Impatto: Un attaccante potrebbe sfruttare questa vulnerabilità per ottenere accesso non autorizzato, eseguire codice arbitrario o compromettere i dati memorizzati nell'applicazione. Questo potrebbe portare alla perdita di dati sensibili o al controllo completo del sistema da parte dell'attaccante.	

Soluzione: Aggiornare Koken alla versione più recente che contiene le patch di sicurezza per risolvere questa vulnerabilità.
Metodo di detection: Vulnerabilità indiviata tramite il software Searchsploit.

JQuery 1.2 < 3.5.0 Multiple XSS	CVE
	CVE-2020-11023
MEDIA	
Descrizione: Le versioni di jQuery dalla 1.2 alla 3.5.0 sono vulnerabili a diverse vulnerabilità di Cross-Site Scripting (XSS). Un attaccante potrebbe sfruttare queste vulnerabilità per iniettare codice JavaScript dannoso in pagine web affidabili.	
Impatto: Un attaccante potrebbe sfruttare queste vulnerabilità per eseguire codice JavaScript arbitrario nel contesto di sicurezza del sito web della vittima, rubando informazioni sensibili o eseguendo ulteriori attacchi.	
Soluzione: Aggiorna JQuery alla versione 3.5.0 o successiva.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

SMB Signing not required	CVE
	CVE-2016-2115
MEDIA	
Descrizione: Il sistema remoto non richiede la firma SMB. Questo potrebbe permettere a un attaccante di eseguire attacchi man-in-the-middle sulle connessioni SMB.	
Impatto: La mancanza di firma SMB può permettere a un attaccante di intercettare e modificare il traffico SMB tra client e server, compromettendo l'integrità e la riservatezza dei dati.	
Soluzione: Configurare il sistema per richiedere la firma SMB, seguendo le linee guida specifiche del sistema operativo in uso.	

Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.

Missing Anti-clickjacking Header	CVE
	-
MEDIA	
Descrizione: L'host remoto ha una o più condivisioni Windows a cui è possibile accedere tramite la rete con le credenziali fornite. A seconda dei diritti di condivisione, potrebbe consentire a un aggressore di leggere/scrivere dati riservati.	
Impatto: Gli utenti potrebbero essere ingannati nel cliccare su elementi nascosti che eseguono azioni dannose a loro insaputa. Questo può portare a compromissioni di sicurezza significative, come la divulgazione di informazioni sensibili o l'esecuzione di azioni non autorizzate.	
Soluzione: I browser Web moderni supportano le intestazioni HTTP Content-Security-Policy e X-Frame-Options. Assicurati che una di queste sia impostata su tutte le pagine Web restituite dal tuo sito/app. Se ti aspetti che la pagina venga inserita in un frame solo da pagine sul tuo server (ad esempio, fa parte di un FRAMESET), allora vorrai usare SAMEORIGIN, altrimenti se non ti aspetti mai che la pagina venga inserita in un frame, dovresti usare DENY. In alternativa, considera di implementare la direttiva "frame-ancestors" della Content Security Policy.	
Metodo di detection: Vulnerabilità indiviata tramite il software OWASP ZAP e Nikto.	

Assenza di token anti-CSRF	CVE
	CVE-2017-14092
MEDIA	
Descrizione: L'applicazione web non implementa token Anti-CSRF (Cross-Site Request Forgery). Questo potrebbe permettere a un attaccante di inviare richieste non autorizzate come se fossero inviate da un utente legittimo.	
Impatto: Gli attaccanti potrebbero sfruttare questa vulnerabilità per eseguire azioni indesiderate a nome degli utenti autenticati, compromettendo l'integrità dei dati e la sicurezza dell'utente.	

Soluzione: Implementare token Anti-CSRF per tutte le operazioni critiche che modificano lo stato dell'applicazione o dei dati.
Metodo di detection: Vulnerabilità indiviata tramite il software OWASP ZAP.

Content Security Policy (CSP) Header Not Set	CVE
	CVE-2018-5164
MEDIA	
Descrizione: L'intestazione HTTP Content Security Policy (CSP) non è configurata. CSP è una difesa efficace contro vari tipi di attacchi come XSS (Cross-Site Scripting).	
Impatto: L'assenza di CSP permette l'iniezione di script dannosi nel contesto dell'utente, aumentando il rischio di attacchi XSS e di altre minacce alla sicurezza.	
Soluzione: Configurare l'intestazione CSP per limitare le fonti di contenuti approvati, riducendo significativamente la superficie di attacco.	
Metodo di detection: Vulnerabilità indiviata tramite il software OWASP ZAP e Nikto.	

Directory Browsing	CVE
	-
MEDIA	
Descrizione: È possibile visualizzare l'elenco delle directory. L'elenco delle directory può rivelare script nascosti, includere file, file di origine del backup, ecc. a cui è possibile accedere per leggere informazioni sensibili.	
Impatto: Gli attaccanti potrebbero raccogliere informazioni su file e directory, facilitando ulteriori attacchi contro il sistema.	
Soluzione: Disabilitare la navigazione delle directory nel file di configurazione del server web.	
Metodo di detection:	

Vulnerabilità indiviata tramite il software OWASP ZAP.

ICMP Timestamp Request Remote Date Disclosure	CVE
	CVE-1999-0524
BASSA	
Descrizione: L'host remoto risponde a una richiesta di timestamp ICMP. Ciò consente a un aggressore di conoscere la data impostata sulla macchina presa di mira, il che può aiutare un aggressore remoto non autenticato a sconfiggere i protocolli di autenticazione basati sul tempo.	
Impatto: Un attaccante potrebbe utilizzare queste informazioni per sincronizzare ulteriori attacchi o per raccogliere informazioni aggiuntive sul sistema remoto.	
Soluzione: Filtrare le richieste di timestamp ICMP (13) e le risposte di timestamp ICMP in uscita (14).	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus ed OpenVas.	

TCP Timestamps Information Disclosure	CVE
	-
BASSA	
Descrizione: La funzionalità di timestamp TCP è abilitata sul sistema remoto. I timestamp TCP possono essere utilizzati per calcolare l'uptime del sistema e l'orario di avvio, fornendo informazioni che possono essere utilizzate per attacchi mirati.	
Impatto: Un effetto collaterale di questa funzionalità è che a volte è possibile calcolare il tempo di attività dell'host remoto.	
Soluzione: Disabilitare i timestamp TCP nel file di configurazione del sistema operativo o applicare le policy di sicurezza raccomandate per limitare l'esposizione di queste informazioni.	
Metodo di detection: Vulnerabilità indiviata tramite il software OpenVas.	

Server Leaks Version Information via "Server" HTTP Response Header Field	CVE
	-
BASSA	
Descrizione: l server Web/applicazione perde informazioni sulla versione tramite l'intestazione della risposta HTTP "Server". L'accesso a tali informazioni può facilitare agli aggressori l'identificazione di altre vulnerabilità a cui è soggetto il server web/applicazione.	
Impatto: La divulgazione delle informazioni sulla versione del server può facilitare la fase di ricognizione di un attaccante, permettendogli di mirare a vulnerabilità note associate alla versione specifica del server web.	
Soluzione: Configurare il server web per non rivelare informazioni sulla versione nel campo dell'intestazione di risposta "Server". Questa pratica può essere realizzata tramite la configurazione del server web o l'uso di moduli di sicurezza.	
Metodo di detection: Vulnerabilità indiviata tramite il software OWASP ZAP.	

X-Content-Type-Options Header Missing	CVE
	CVE-2019-19089
BASSA	
Descrizione: L'intestazione HTTP X-Content-Type-Options non è configurata. Questa intestazione aiuta a prevenire attacchi di tipo MIME-sniffing, indicando ai browser di non cambiare il tipo di contenuto dichiarato del MIME e di rispettare il tipo di contenuto definito nel Content-Type.	
Impatto: L'assenza dell'intestazione X-Content-Type-Options può permettere a un attaccante di eseguire attacchi di MIME-sniffing, inducendo il browser a trattare i file come tipi di contenuto diversi da quelli dichiarati. Questo può portare a esecuzione di script dannosi o download di file pericolosi.	
Soluzione: Configurare l'intestazione X-Content-Type-Options con il valore "nosniff" su tutte le risposte HTTP del server per prevenire questi attacchi.	
Metodo di detection: Vulnerabilità indiviata tramite il software OWASP ZAP.	

Cross-Domain JavaScript Source File Inclusion	CVE
	-
BASSA	
Descrizione: L'applicazione web include file JavaScript da domini esterni. Questa pratica può esporre l'applicazione a rischi di sicurezza, poiché il contenuto dei file esterni può essere modificato dall'attaccante per eseguire codice dannoso.	
Impatto: Gli attaccanti potrebbero sfruttare questa vulnerabilità per iniettare codice JavaScript dannoso nell'applicazione, rubare dati sensibili degli utenti, eseguire attacchi di Cross-Site Scripting (XSS) o compromettere ulteriormente il sistema.	
Soluzione: Evitare di includere file JavaScript da domini esterni a meno che non siano strettamente necessari. In alternativa, assicurarsi che i file inclusi siano da fonti affidabili e considerare l'uso di Subresource Integrity (SRI) per verificare l'integrità dei file esterni.	
Metodo di detection: Vulnerabilità indiviata tramite il software OWASP ZAP.	

Server Leaks Version Information via "Server" HTTP Response Header Field	CVE
	-
BASSA	
Descrizione: Il server Web/applicazione perde informazioni sulla versione tramite l'intestazione della risposta HTTP "Server". L'accesso a tali informazioni può facilitare agli aggressori l'identificazione di altre vulnerabilità a cui è soggetto il server web/applicazione.	
Impatto: La divulgazione delle informazioni sulla versione del server può facilitare la fase di ricognizione di un attaccante, permettendogli di mirare a vulnerabilità note associate alla versione specifica del server web.	
Soluzione: Configurare il server web per non rivelare informazioni sulla versione nel campo dell'intestazione di risposta "Server". Questa pratica può essere realizzata tramite la configurazione del server web o l'uso di moduli di sicurezza.	
Metodo di detection: Vulnerabilità indiviata tramite il software OWASP ZAP.	

Apache Banner Linux Distribution Disclosure	CVE
	-
INFORMATIVA	
Descrizione: Il banner di Apache su questo sistema Linux rivela la distribuzione in uso. Questa informazione può essere utilizzata da un attaccante per identificare potenziali vulnerabilità specifiche della distribuzione.	
Impatto: La divulgazione della distribuzione Linux può facilitare la fase di ricognizione per un attaccante, permettendogli di mirare a vulnerabilità specifiche della distribuzione.	
Soluzione: Configurare il server web per non rivelare informazioni sulla distribuzione nel banner di Apache.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Apache HTTP Server Version	CVE
	-
INFORMATIVA	
Descrizione: Il server Apache HTTP su questo sistema rivela la versione in uso. Questa informazione può essere utilizzata da un attaccante per identificare potenziali vulnerabilità specifiche della versione.	
Impatto: La divulgazione della versione del server Apache HTTP può facilitare la fase di ricognizione per un attaccante, permettendogli di mirare a vulnerabilità specifiche della versione.	
Soluzione: Configurare il server web per non rivelare informazioni sulla versione di Apache HTTP nel banner.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus e Nitko2.	

Backported Security Patch Detection (WWW)	CVE
	-
INFORMATIVA	
Descrizione: Il sistema ha rilevato patch di sicurezza backportate per il server web. Queste patch possono includere correzioni di sicurezza senza modificare il numero di versione del software.	
Impatto: Le patch di sicurezza backportate possono aiutare a mantenere la sicurezza del sistema senza dover eseguire aggiornamenti completi del software. Tuttavia, la mancata visibilità delle versioni corrette potrebbe confondere i controlli di sicurezza automatizzati.	
Soluzione: Verificare regolarmente la disponibilità di patch di sicurezza e applicarle tempestivamente per garantire la protezione contro le vulnerabilità note.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Common Platform Enumeration (CPE)	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva e segnala le informazioni CPE (Common Platform Enumeration) associate ai software e ai sistemi rilevati durante la scansione.	
Impatto: L'utilizzo di CPE consente una gestione più precisa delle risorse IT e delle vulnerabilità associate.	
Soluzione: Utilizzare le informazioni CPE per valutare e gestire le vulnerabilità presenti nel sistema, assicurandosi che tutte le patch rilevanti siano applicate.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Device Type	CVE
	-
INFORMATIVA	
Descrizione:	

Questo plugin rileva il tipo di dispositivo (ad esempio, router, switch, server, ecc.) basato sulle informazioni raccolte durante la scansione.
Impatto: La conoscenza del tipo di dispositivo può aiutare a pianificare attacchi mirati o a gestire meglio le risorse di rete.
Soluzione: Utilizzare le informazioni sul tipo di dispositivo per migliorare la gestione della sicurezza e assicurarsi che tutti i dispositivi siano configurati e protetti correttamente.
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.

Ethernet Card Manufacturer Detection	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva il produttore delle schede di rete Ethernet presenti su un host remoto.	
Impatto: Le informazioni sul produttore delle schede di rete possono essere utilizzate per identificare potenziali vulnerabilità specifiche del hardware di rete.	
Soluzione: Assicurarsi che i driver e il firmware delle schede di rete siano aggiornati con le ultime patch di sicurezza.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Ethernet MAC Addresses	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva gli indirizzi MAC delle schede di rete presenti su un host remoto.	
Impatto: Le informazioni sugli indirizzi MAC possono essere utilizzate per identificare e monitorare dispositivi specifici sulla rete.	
Soluzione:	

Utilizzare le informazioni sugli indirizzi MAC per gestire e monitorare la rete in modo efficace, applicando politiche di sicurezza appropriate.
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.

HTTP Methods Allowed (per directory)	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva i metodi HTTP consentiti per ciascuna directory su un server web.	
Impatto: La conoscenza dei metodi HTTP consentiti può aiutare a identificare configurazioni non sicure e potenziali vettori di attacco.	
Soluzione: Configurare il server web per limitare i metodi HTTP solo a quelli necessari, seguendo le migliori pratiche di sicurezza.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

HTTP Server Type and Version	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva il tipo e la versione del server HTTP in uso su un host remoto.	
Impatto: La conoscenza del tipo e della versione del server HTTP può aiutare un attaccante a pianificare attacchi mirati sfruttando vulnerabilità note.	
Soluzione: Assicurarsi che il server HTTP sia aggiornato con le ultime patch di sicurezza e configurato secondo le migliori pratiche di sicurezza.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Host Fully Qualified Domain Name (FQDN) Resolution	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva la risoluzione del nome di dominio completamente qualificato (FQDN) per un host remoto.	
Impatto: La conoscenza del FQDN può aiutare nella gestione della rete e nell'identificazione di risorse specifiche.	
Soluzione: Utilizzare le informazioni sul FQDN per migliorare la gestione delle risorse di rete e la sicurezza del sistema.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

HyperText Transfer Protocol (HTTP) Information	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin raccoglie informazioni sui server HTTP rilevati, inclusi header, cookie e altri dettagli di configurazione.	
Impatto: Le informazioni raccolte possono essere utilizzate per identificare potenziali vulnerabilità e migliorare la configurazione di sicurezza del server HTTP.	
Soluzione: Utilizzare le informazioni raccolte per configurare il server HTTP in modo sicuro e applicare le patch di sicurezza necessarie.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

JQuery Detection	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva l'uso della libreria JavaScript JQuery su un host remoto. Queste informazioni possono essere utilizzate per identificare potenziali vulnerabilità nella versione di JQuery in uso.	

Impatto: La conoscenza dell'uso di JQuery può aiutare un attaccante a pianificare attacchi mirati sfruttando vulnerabilità note della libreria.
Soluzione: Assicurarsi di utilizzare l'ultima versione stabile di JQuery e mantenere aggiornate le librerie per mitigare i rischi di sicurezza.
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.

Microsoft Windows SMB: Obtains the Password Policy	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin utilizza SMB per ottenere le informazioni sulla politica delle password su una macchina Windows.	
Impatto: La conoscenza della politica delle password può aiutare un attaccante a pianificare attacchi mirati, come attacchi di forza bruta.	
Soluzione: Limitare l'accesso alle informazioni sulla politica delle password e applicare politiche di sicurezza rigorose per proteggere questi dati.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Microsoft Windows SMB LsaQueryInformationPolicy Function SID Enumeration	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin utilizza la funzione LsaQueryInformationPolicy di SMB per enumerare gli SID (Security Identifier) su una macchina Windows.	
Impatto: La conoscenza degli SID può aiutare un attaccante a pianificare attacchi mirati sfruttando vulnerabilità specifiche.	
Soluzione: Limitare l'accesso alla funzione LsaQueryInformationPolicy e applicare politiche di sicurezza rigorose per proteggere questi dati.	
Metodo di detection:	

Vulnerabilità indiviata tramite il software Nessus.

Microsoft Windows SMB NativeLanManager Remote System Information Disclosure	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva la divulgazione di informazioni di sistema tramite SMB NativeLanManager su una macchina WindowsEcco le descrizioni aggiornate per le vulnerabilità elencate, basate sulle informazioni fornite da Tenable:	
Impatto: La divulgazione di informazioni di sistema può aiutare un attaccante a raccogliere dati utili per pianificare attacchi mirati o sfruttare vulnerabilità specifiche del sistema.	
Soluzione: Configurare il sistema per limitare la divulgazione di informazioni sensibili tramite il protocollo SMB e implementare misure di sicurezza per proteggere i dati di sistema.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Microsoft Windows SMB Service Detection	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva la presenza di servizi SMB attivi su un host remoto. Queste informazioni possono essere utilizzate per identificare le configurazioni di rete e i servizi in esecuzione.	
Impatto: La conoscenza dei servizi SMB attivi può aiutare un attaccante a pianificare attacchi mirati sfruttando vulnerabilità note dei servizi identificati.	
Soluzione: Configurare i servizi SMB in modo sicuro, applicare regolarmente le patch di sicurezza e limitare l'accesso ai servizi critici solo agli utenti autorizzati.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Microsoft Windows SMB Share Permissions Enumeration	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva le autorizzazioni di condivisione SMB su una macchina Windows. Queste informazioni possono essere utilizzate per identificare configurazioni non sicure e potenziali punti di accesso per attacchi.	
Impatto: La conoscenza delle autorizzazioni di condivisione SMB può aiutare un attaccante a identificare punti deboli nella configurazione di sicurezza e a pianificare attacchi mirati.	
Soluzione: Verificare e configurare le autorizzazioni di condivisione SMB in modo sicuro, limitando l'accesso solo agli utenti autorizzati e applicando le migliori pratiche di sicurezza.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Microsoft Windows SMB Shares Enumeration	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva le condivisioni SMB attive su una macchina Windows. Queste informazioni possono essere utilizzate per identificare risorse di rete condivise e potenziali punti di accesso per attacchi.	
Impatto: La conoscenza delle condivisioni SMB attive può aiutare un attaccante a identificare risorse vulnerabili e a pianificare attacchi mirati.	
Soluzione: Verificare e configurare le condivisioni SMB in modo sicuro, limitando l'accesso solo agli utenti autorizzati e applicando le migliori pratiche di sicurezza.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Microsoft Windows SMB Versions Supported (remote check)	CVE
	-

INFORMATIVA
Descrizione: Questo plugin rileva le versioni del protocollo SMB supportate su un host remoto. Queste informazioni possono essere utilizzate per identificare potenziali vulnerabilità specifiche delle versioni di SMB rilevate.
Impatto: La conoscenza delle versioni SMB supportate può aiutare un attaccante a pianificare attacchi mirati sfruttando vulnerabilità specifiche delle versioni identificate.
Soluzione: Assicurarsi che SMB sia aggiornato con le ultime patch di sicurezza e configurato secondo le migliori pratiche di sicurezza.
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.

Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva i dialetti SMB2 e SMB3 supportati su un host remoto. Queste informazioni possono essere utilizzate per identificare potenziali vulnerabilità specifiche delle versioni di SMB rilevate.	
Impatto: La conoscenza dei dialetti SMB2 e SMB3 supportati può aiutare un attaccante a pianificare attacchi mirati sfruttando vulnerabilità specifiche delle versioni identificate.	
Soluzione: Assicurarsi di utilizzare le versioni più recenti e sicure di SMB e applicare regolarmente le patch di sicurezza per mitigare i rischi associati alle vulnerabilità note.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Nessus SYN scanner	CVE
	-
INFORMATIVA	

Descrizione: Questo plugin è uno scanner di porte "half-open" SYN. È relativamente veloce anche contro target con firewall. Le scansioni SYN sono meno intrusive rispetto alle scansioni TCP complete, ma possono causare problemi a firewall meno robusti e lasciare connessioni non chiuse sul target remoto se la rete è molto trafficata.
Impatto: La scansione SYN può essere utilizzata per identificare i servizi in esecuzione su un host remoto, che può essere utile per pianificare ulteriori verifiche di sicurezza o attacchi mirati.
Soluzione: Proteggere il target con un filtro IP.
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.

Nessus Scan Information	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin raccoglie informazioni dettagliate sulla scansione effettuata con Nessus, inclusi dettagli sugli host scansionati, i plugin utilizzati e i risultati della scansione.	
Impatto: Le informazioni sulla scansione possono essere utilizzate per analizzare la sicurezza di un sistema e pianificare miglioramenti basati sui risultati ottenuti.	
Soluzione: Utilizzare le informazioni raccolte per migliorare la configurazione di sicurezza del sistema e risolvere le vulnerabilità identificate.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

OS Identification	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin identifica il sistema operativo in uso su un host remoto. Queste informazioni possono essere utilizzate per determinare potenziali vulnerabilità specifiche del sistema operativo identificato.	
Impatto:	

La conoscenza del sistema operativo può aiutare un attaccante a pianificare attacchi mirati sfruttando vulnerabilità note associate a quel sistema operativo
Soluzione: Assicurarsi che il sistema operativo sia aggiornato con le ultime patch di sicurezza e configurato secondo le migliori pratiche di sicurezza.
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.

Patch Report	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin genera un report sulle patch di sicurezza applicate e mancanti su un host remoto. Questo report può essere utilizzato per valutare la conformità del sistema alle politiche di sicurezza.	
Impatto: Un report sulle patch può aiutare a identificare le aree del sistema che richiedono aggiornamenti di sicurezza e a pianificare azioni malevoli.	
Soluzione: Installare le patch mancanti.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

SMB Use Host SID to Enumerate Local Users	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin utilizza l'host SID di SMB per enumerare gli utenti locali su una macchina Windows. Queste informazioni possono essere utilizzate per identificare account utente e pianificare attacchi di forza bruta o altre attività malevole.	
Impatto: La conoscenza degli utenti locali può aiutare un attaccante a identificare account target e a pianificare ulteriori attacchi di compromissione.	
Soluzione: Limitare l'accesso alle funzioni di enumerazione di SMB e implementare politiche di sicurezza rigorose per proteggere le informazioni sugli account utente.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Samba Server Detection	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva la presenza di un server Samba in esecuzione su una macchina. Samba è un software che fornisce servizi di condivisione di file e stampanti su reti con sistemi operativi diversi.	
Impatto: La rilevazione di un server Samba può essere utilizzata per pianificare attacchi mirati contro le risorse condivise e per sfruttare eventuali vulnerabilità note del software Samba.	
Soluzione: Assicurarsi che il server Samba sia configurato in modo sicuro e che le patch di sicurezza siano applicate regolarmente. Limitare l'accesso alle risorse condivise solo agli utenti autorizzati.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Samba Version	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva la versione di Samba in uso su un host remoto. Queste informazioni possono essere utilizzate per identificare potenziali vulnerabilità specifiche della versione di Samba rilevata	
Impatto: La conoscenza della versione di Samba può aiutare un attaccante a pianificare attacchi mirati sfruttando vulnerabilità note associate a quella versione.	
Soluzione: Assicurarsi che Samba sia aggiornato con le ultime patch di sicurezza e configurato secondo le migliori pratiche di sicurezza.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)	CVE
	-

INFORMATIVA	
Descrizione: Questo plugin rileva che la versione 1 del protocollo SMB è abilitata su un host remoto. SMBv1 è noto per avere numerose vulnerabilità di sicurezza e il suo utilizzo è sconsigliato.	
Impatto: L'utilizzo di SMBv1 espone il sistema a rischi elevati di sicurezza, inclusi attacchi di esecuzione di codice remoto e compromissione dei dati.	
Soluzione: Disabilitare SMBv1 e utilizzare versioni più recenti e sicure del protocollo SMB, come SMBv2 o SMBv3.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Service Detection	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva i servizi in esecuzione su un host remoto. Queste informazioni possono essere utilizzate per identificare le applicazioni e i servizi attivi e per valutare la superficie di attacco del sistema.	
Impatto: La conoscenza dei servizi in esecuzione può aiutare un attaccante a pianificare attacchi mirati sfruttando vulnerabilità note dei servizi identificati.	
Soluzione: Configurare i servizi in modo sicuro, applicare regolarmente le patch di sicurezza e limitare l'accesso ai servizi critici solo agli utenti autorizzati.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

TCP/IP Timestamps Supported	CVE
	-
INFORMATIVA	
Descrizione:	

Questo plugin rileva che i timestamp TCP/IP sono abilitati su un host remoto. I timestamp TCP/IP possono essere utilizzati per calcolare l'uptime del sistema e l'orario di avvio, fornendo informazioni che possono essere utilizzate per attacchi mirati.
Impatto: Un attaccante potrebbe utilizzare i timestamp TCP/IP per stimare l'orario di avvio del sistema e l'uptime, informazioni che possono essere sfruttate per pianificare attacchi o per analisi forensi in caso di compromissione del sistema.
Soluzione: Disabilitare i timestamp TCP/IP nel file di configurEcco le descrizioni aggiornate utilizzando le informazioni trovate sul sito di Tenable per le vulnerabilità elencate:
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.

Traceroute Information	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin raccoglie informazioni tramite traceroute per determinare il percorso dei pacchetti fino a un host remoto. Queste informazioni possono includere dettagli sui router intermedi e sui tempi di risposta.	
Impatto: Le informazioni di traceroute possono aiutare un attaccante a mappare la rete e a identificare potenziali punti di attacco o di interdizione.	
Soluzione: Limitare l'accesso agli strumenti di diagnostica di rete solo agli utenti autorizzati e monitorare l'attività di rete per rilevare tentativi non autorizzati di mappatura della rete.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Unix Operating System on Extended Support	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva un sistema operativo Unix che è ancora in supporto esteso. Questo significa che il sistema operativo riceve solo aggiornamenti di sicurezza critici e non nuove funzionalità.	
Impatto: L'uso di un sistema operativo in supporto esteso può limitare la capacità di aggiornare il sistema con nuove funzionalità e miglioramenti di sicurezza, aumentando il rischio di esposizione a vulnerabilità.	
Soluzione: Pianificare l'aggiornamento a una versione più recente del sistema operativo che sia pienamente supportata e che riceva aggiornamenti regolari.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

VMware Virtual Machine Detection	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva che l'host remoto è una macchina virtuale VMware. Questa informazione può essere utilizzata per identificare l'ambiente di virtualizzazione in uso.	
Impatto: La conoscenza dell'ambiente di virtualizzazione può aiutare un attaccante a pianificare attacchi specifici per l'hypervisor o per le configurazioni di sicurezza della macchina virtuale.	
Soluzione: Assicurarsi che l'ambiente di virtualizzazione sia configurato in modo sicuro e che le patch di sicurezza siano applicate regolarmente.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

WMI Not Available	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva che Windows Management Instrumentation (WMI) non è disponibile sull'host remoto. WMI è utilizzato per gestire e monitorare i sistemi Windows.	
Impatto: L'indisponibilità di WMI può limitare la capacità di monitorare e gestire il sistema in modo efficace, aumentando il rischio di non rilevare problemi di sicurezza o di prestazioni.	
Soluzione: Assicurarsi che WMI sia abilitato e correttamente configurato sull'host remoto per permettere una gestione e un monitoraggio efficaci.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Web Server No 404 Error Code Check	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva che il server web non restituisce il codice di errore 404 quando una risorsa non viene trovata. Questo comportamento può essere utilizzato per nascondere l'esistenza di risorse o directory specifiche.	
Impatto: La mancanza di un codice di errore 404 può confondere gli utenti legittimi e i motori di ricerca, rendendo più difficile diagnosticare problemi e migliorare l'esperienza utente.	
Soluzione: Configurare il server web per restituire il codice di errore 404 quando una risorsa non viene trovata e per gestire correttamente gli errori HTTP.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

	CVE

Windows NetBIOS / SMB Remote Host Information Disclosure	-
INFORMATIVA	
Descrizione: Questo plugin rileva che l'host remoto divulga informazioni tramite NetBIOS/SMB. Queste informazioni possono includere dettagli sul nome dell'host, il dominio e altre configurazioni di rete.	
Impatto: La divulgazione di informazioni tramite NetBIOS/SMB può aiutare un attaccante a raccogliere dati utili per pianificare attacchi mirati o per sfruttare vulnerabilità specifiche del sistema.	
Soluzione: Limitare la divulgazione di informazioni tramite NetBIOS/SMB e implementare politiche di sicurezza per proteggere i dati di rete.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

mDNS Detection (Local Network)	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva l'uso di mDNS (Multicast DNS) sulla rete locale. mDNS è utilizzato per risolvere i nomi host in indirizzi IP senza la necessità di un server DNS centralizzato.	
Impatto: L'uso di mDNS può facilitare la scoperta di dispositivi sulla rete locale, ma può anche esporre il sistema a rischi di sicurezza se non configurato correttamente.	
Soluzione: Assicurarsi che mDNS sia configurato in modo sicuro e limitare la sua portata solo ai dispositivi e alle reti di fiducia.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

GET for POST	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva l'uso improprio del metodo HTTP GET al posto di POST in richieste che dovrebbero utilizzare POST per garantire la sicurezza.	
Impatto: L'uso improprio del metodo GET per inviare dati sensibili può esporre queste informazioni a intercettazioni o manipolazioni, poiché i parametri inviati tramite GET sono visibili nell'URL.	
Soluzione: Configurare l'applicazione web per utilizzare correttamente il metodo POST per tutte le richieste che inviano dati sensibili o che modificano lo stato del server.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

User Controllable HTML Element Attribute (Potential XSS)	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin rileva che un attributo di un elemento HTML è controllabile dall'utente, il che potrebbe essere sfruttato per attacchi di Cross-Site Scripting (XSS).	
Impatto: Se un attributo HTML controllabile dall'utente non sanitizzasse adeguatamente, un attaccante potrebbe iniettare codice JavaScript dannoso che verrebbe eseguito nel contesto del browser della vittima.	
Soluzione: Implementare misure di sanitizzazione e validazione degli input per tutti gli attributi HTML controllabili dall'utente per prevenire attacchi XSS.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

User Agent Fuzzer	CVE
	-
INFORMATIVA	
Descrizione:	

Questo plugin testa l'applicazione web inviando richieste con user agent modificati per rilevare potenziali vulnerabilità nella gestione degli user agent.
Impatto: Una gestione inadeguata degli user agent può portare a vulnerabilità di sicurezza, come attacchi di SQL Injection o Cross-Site Scripting (XSS).
Soluzione: Assicurarsi che l'applicazione web gestisca correttamente e sanitizzi tutti gli input degli user agent.
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.

Modern Web Application	CVE
	-
INFORMATIVA	
Descrizione: Questo plugin identifica caratteristiche e framework tipici delle moderne applicazioni web, come l'uso di AJAX, HTML5, e altre tecnologie avanzate.	
Impatto: Conoscere le tecnologie utilizzate in un'applicazione web può aiutare un attaccante a identificare potenziali vettori di attacco specifici per quei framework o tecnologie.	
Soluzione: Mantenere aggiornati i framework e le tecnologie utilizzate nell'applicazione web e applicare le migliori pratiche di sicurezza per ciascuno di essi.	
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.	

Information Disclosure - Suspicious Comments	**CVE**
	-
INFORMATIVA	
Descrizione: Questo plugin rileva commenti sospetti o informativi nel codice sorgente HTML di un'applicazione web. Questi commenti possono rivelare informazioni sensibili o dettagli di implementazione.	
Impatto:	

I commenti nel codice sorgente possono fornire indizi su come funziona l'applicazione, facilitando potenzialmente attacchi mirati o sfruttamento di vulnerabilità.
Soluzione: Rimuovere o mascherare i commenti sospetti o informativi nel codice sorgente HTML e mantenere una buona igiene del codice.
Metodo di detection: Vulnerabilità indiviata tramite il software Nessus.

Appendix

Una dimostrazione di come è stata sfruttata le vulnerabilita è documentata nel documento PenetrationTesting Metodologie, disponible anche al link:

https://github.com/D-DiSarno/Penetration_Testing-Photographer-1

```
www-data@photographer:/home$ ls daisa
ls daisa
Desktop    Downloads  Pictures  Templates  examples.desktop
Documents  Music      Public    Videos     user.txt
www-data@photographer:/home$ cat daisa/user.txt
cat daisa/user.txt
d41d8cd98f00b204e9800998ecf8427e
```

Figura 4: Prima bandiera catturata

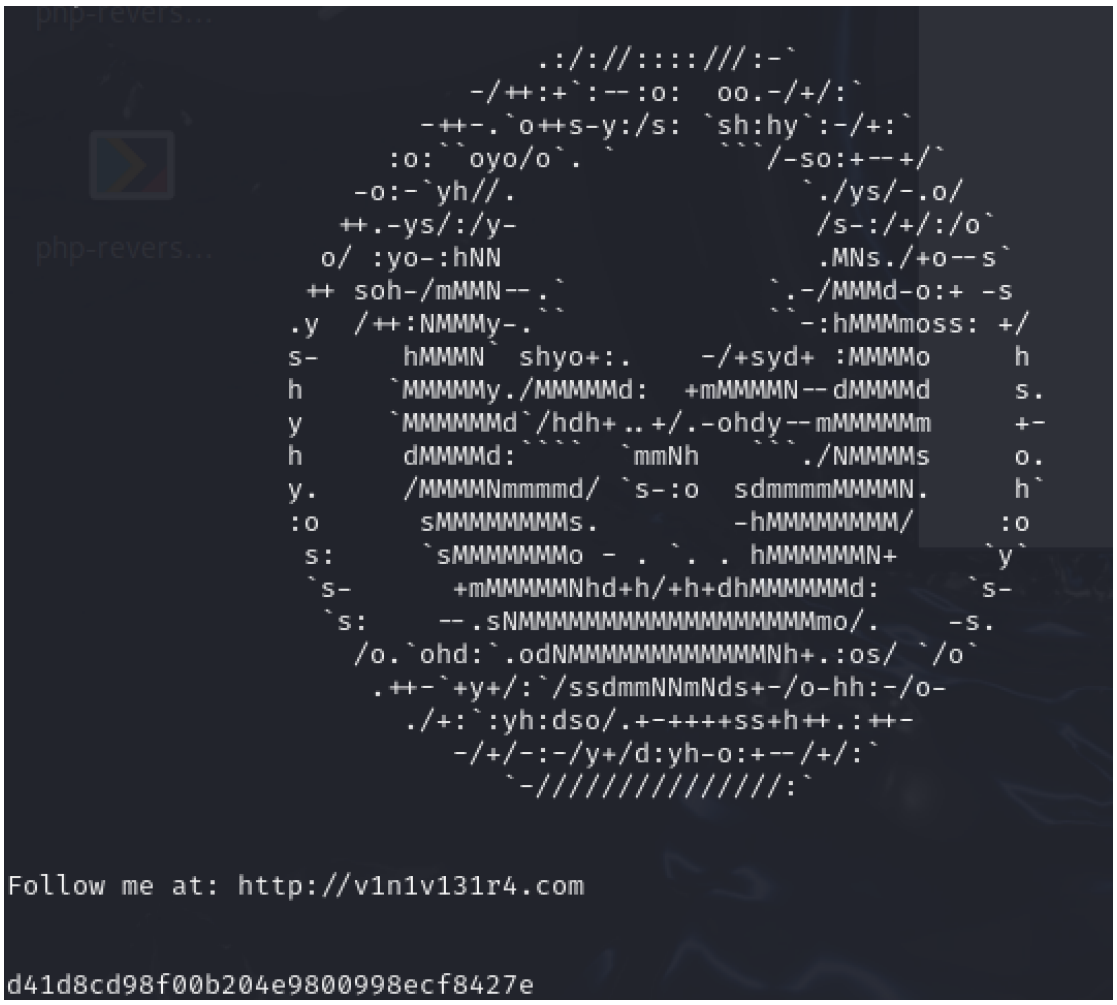

Figura 5: Seconda bandiera catturata

References

- CVE-2020-11023: https://nvd.nist.gov/vuln/detail/CVE-2020-11023
- Koken: Vulnerabilità nella versione 0.22.24: https://www.exploit-db.com/exploits/48706
- CVE-2016-2115: https://nvd.nist.gov/vuln/detail/CVE-2016-2115
- CVE-2017-14092: https://nvd.nist.gov/vuln/detail/CVE-2017-14092
- CVE-2018-5164: https://nvd.nist.gov/vuln/detail/CVE-2018-5164
- CVE-1999-0524: https://nvd.nist.gov/vuln/detail/CVE-1999-0524
- CVE-2019-19089: https://nvd.nist.gov/vuln/detail/CVE-2019-19089