Università degli Studi di Salerno

Penetration Testing Report

INFERNO 1.1

Mario Lezzi | Corso di PTEH | A.A. 2024/2025

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Sommario

1. Executive Summary

Lo studente Mario Lezzi ha condotto un'attività di Penetration Testing sull'asset virtuale denominato **Inferno 1.1**, disponibile su VulnHub [1], con l'obiettivo di identificarne le vulnerabilità e valutare il livello complessivo di sicurezza. L'asset oggetto dell'analisi consiste in una macchina virtuale posizionata all'interno di una rete isolata, raggiungibile all'indirizzo IP **10.0.2.6**.

Il test ha previsto l'analisi dei servizi esposti e degli applicativi attivi, con particolare attenzione alla web application erogata attraverso la porta 80. Non è stata fornita alcuna credenziale o informazione preliminare sul sistema, motivo per cui si è optato per una valutazione di tipo **black-box**. L'attività è stata svolta tra il 5 Giugno 2025 e il 25 Giugno 2025.

Durante l'attività sono state individuate vulnerabilità e configurazioni insicure che compromettono seriamente la sicurezza complessiva del sistema. In particolare, è stato possibile ottenere accesso remoto non autorizzato tramite sfruttamento di un'applicazione web vulnerabile, per poi eseguire una escalation dei privilegi fino ad ottenere pieno controllo della macchina con privilegi di root.

Tra le problematiche principali si evidenziano l'utilizzo di software obsoleto, la mancanza di aggiornamenti di sicurezza, e la presenza di una configurazione sudo eccessivamente permissiva, che consente l'esecuzione di comandi privilegiati senza richiesta di password. Tali condizioni rendono l'asset facilmente compromettibile anche da parte di un attaccante privo di credenziali, con un rischio operativo estremamente elevato.

L'adozione delle adeguate contromisure proposte nel capitolo *"Remediation Report"* consentirebbe di ridurre sensibilmente il rischio di compromissione e migliorare la sicurezza complessiva dell'asset.

2. Engagement Highlights

L'attività di Penetration Testing è stata svolta nell'ambito del corso universitario "Penetration Testing & Ethical Hacking", con finalità esclusivamente didattiche. Il committente formale è il prof. Arcangelo Castiglione, docente titolare del corso presso l'Università degli Studi di Salerno.

Prima dell'avvio delle attività, è stato stabilito un accordo tra le parti coinvolte contenente le Regole di Ingaggio, che includevano:

- **Finalità dell'attività**: esclusivamente formativa e non commerciale.
- **Periodo di esecuzione**: dal 5 Giugno 2025 al 25 Giugno 2025.
- **Ambito dell'analisi**: asset "Inferno 1.1" installato in ambiente isolato, IP 10.0.2.6.
- **Metodologia adottata**: libera scelta delle tecniche offensive ritenute utili ai fini formativi, ad eccezione del social engineering, escluso in quanto l'asset non coinvolge soggetti umani.
- **Accordo di non divulgazione (NDA)**: i risultati dell'attività, nonché le eventuali informazioni raccolte, saranno trattati con riservatezza e condivisi esclusivamente con il docente al fine della valutazione accademica.
- **Budget e costi**: trattandosi di un'attività didattica, non è previsto alcun compenso. Eventuali costi accessori sono a carico dello studente.

A fini didattici e al fine di valutare il reale livello di rischio dell'asset, è stata concessa l'autorizzazione all'uso delle seguenti tecniche:

1. Scoperta, analisi e sfruttamento delle vulnerabilità rilevate per ottenere accesso non autorizzato al sistema target.
2. Tecniche di password cracking per valutare la robustezza delle credenziali eventualmente presenti.
3. In caso di accesso riuscito:
    - tecniche di post-exploitation per l'esplorazione della macchina compromessa e dei dati disponibili;

- privilege escalation per ottenere accesso ad account con maggiori privilegi;
- installazione di backdoor o web shell a scopo dimostrativo, al fine di evidenziare i rischi di persistenza di un attaccante nel sistema;
- raccolta di informazioni critiche per evidenziare potenziali impatti sulla riservatezza o sull'integrità del sistema.

Tutte le attività sono state svolte nel rispetto dei limiti concordati, senza arrecare danni intenzionali o modifiche permanenti alla configurazione dell'asset.

2.1 Risultati attesi

Al termine dell'attività, lo studente dovrà produrre i seguenti elaborati:

- un Documento di Replicabilità tecnico-operativo;
- un Penetration Test Report strutturato secondo le linee guida didattiche;
- una presentazione digitale a supporto della discussione orale.

Tutti i materiali saranno consegnati al prof. Arcangelo Castiglione entro i termini previsti per la valutazione finale del modulo.

3. Vulnerability Report

Durante il processo sono state individuate diverse vulnerabilità. Di seguito sono elencate le principali:

- L'asset espone un'interfaccia web basata su un ambiente di sviluppo accessibile da browser. Questa componente è affetta da una vulnerabilità nota che può compromette la sicurezza complessiva, permettendo a un utente esterno di eseguire operazioni non autorizzate.
- Il sistema consente l'accesso utilizzando credenziali troppo semplici o facilmente intuibili. Questa debolezza può permettere a un attaccante di indovinare nome utente e password con strumenti automatici, ottenendo così accesso non autorizzato all'ambiente.
- All'interno del sistema sono presenti file contenenti credenziali salvate in chiaro. Un soggetto con accesso locale potrebbe leggerle e utilizzarle ottenere accesso ad altri account o risorse del sistema.
- Il sistema è configurato in modo tale da consentire a un utente locale di eseguire operazioni sensibili senza dover inserire la password. Questo comportamento può facilitare l'ottenimento del pieno controllo da parte di un attaccante.
- Il sistema web presenta una debolezza che lo rende vulnerabile a tentativi di manipolazione dell'interfaccia grafica da parte di utenti esterni, con il rischio che l'utente venga indotto a compiere azioni non intenzionali.
- Alcune impostazioni mancanti nel sito web possono indurre i browser a interpretare i contenuti in modo non previsto, con potenziali rischi per l'integrità e la sicurezza delle pagine visitate.
- Il sito non impone regole che limitano l'esecuzione di contenuti da fonti esterne. Questa mancanza rende più facile l'inserimento di codice indesiderato all'interno delle pagine web.
- Il server rivela pubblicamente il tipo e la versione del software utilizzato. Queste informazioni possono essere sfruttate per identificare eventuali punti deboli noti.
- Il sistema utilizza meccanismi di identificazione dei file che espongono dettagli interni, potenzialmente utili a chi vuole analizzare la struttura e i contenuti del server.

- Il software del server è obsoleto e non riceve più aggiornamenti di sicurezza. Questo comporta un rischio elevato, poiché vulnerabilità già note possono essere sfruttate facilmente.
- Il server è configurato per accettare richieste HTTP non strettamente necessarie. Queste funzionalità, se non controllate, possono fornire informazioni aggiuntive utili a un attaccante.
- È presente una vulnerabilità nella gestione delle connessioni sicure (SSH), che può compromettere la riservatezza e l'integrità delle comunicazioni.
- Il sistema risponde a richieste che rivelano l'ora esatta del dispositivo. Queste informazioni possono essere sfruttate per sincronizzare o potenziare altri tipi di attacco.
- Il sistema operativo installato ha raggiunto la fine del suo ciclo di vita e non riceve più aggiornamenti ufficiali. Di conseguenza, è più esposto a rischi noti e non corretti.
- Alcuni componenti critici del sistema utilizzano meccanismi di cifratura considerati deboli o superati, con un impatto negativo sulla protezione dei dati.
- Un componente di rete presenta una debolezza che, in determinate condizioni, può consentire a un utente malintenzionato di eseguire operazioni non autorizzate sul sistema.
- Il modulo mod_session di Apache ha un bug che può causare esecuzione di codice o crash. Può portare al blocco del servizio o a un'escalation di privilegi.
- Il modulo mod_ssl di Apache permette di bypassare i controlli di accesso. L'attaccante può causare un denial of service del server web.
- Il modulo mod_auth_digest contiene un errore che consente un overflow. Potrebbe essere sfruttato per bloccare il server o eseguire codice malevolo.
- Un errore di sincronizzazione nel modulo mod_auth_digest consente di bypassare l'autenticazione.

4. Remediation Report

Di seguito vengono elencate le principali misure correttive consigliate, al fine di migliorare significativamente la postura di sicurezza dell'asset analizzato.

1. **Aggiornare il sistema operativo e i servizi principali**. È fortemente raccomandato migrare verso versioni aggiornate e supportate di Debian, Apache e OpenSSH, in modo da beneficiare di aggiornamenti di sicurezza attivi e patch correttive.
2. **Rimuovere la regola NOPASSWD dal file sudoers**. Limitare l'uso del comando 'sudo' a profili autorizzati, imponendo sempre l'inserimento della password, al fine di prevenire escalation non autorizzate.
3. **Disabilitare l'accesso pubblico all'IDE Codiad o proteggerlo tramite autenticazione forte**. L'esposizione diretta dell'IDE rappresenta un rischio critico. È necessario disabilitare l'accesso esterno oppure isolarlo con misure di accesso controllato.
4. **Implementare configurazioni di sicurezza lato web**. Inserire intestazioni HTTP di sicurezza come Content-Security-Policy, X-Frame-Options, X-Content-Type-Options per ridurre il rischio di manipolazioni lato client. Questi accorgimenti proteggono l'integrità e la riservatezza dell'interazione utente-sito.
5. **Rimuovere credenziali in chiaro presenti nel sistema.** Le credenziali devono essere archiviate in forma cifrata e accessibili solo agli utenti autorizzati, riducendo il rischio di uso improprio.
6. **Rivedere la configurazione del servizio SSH**. Disabilitare algoritmi crittografici obsoleti e assicurarsi che solo standard di cifratura sicuri siano supportati dal servizio.
7. **Limitare la visibilità dei file di default e delle intestazioni del web server.** Informazioni esposte come intestazioni HTTP (Server, ETag) o file di default possono agevolare la ricognizione da parte di attaccanti. È raccomandato rimuoverle o anonimizzarle ove possibile.
8. **Disabilitare funzionalità HTTP non strettamente necessarie.** I metodi superflui vanno disabilitati per ridurre la superficie d'attacco.
9. **Rafforzare le policy di autenticazione.** È consigliabile adottare criteri più restrittivi per la definizione delle credenziali, imponendo l'uso di password complesse e difficili da indovinare.

10. **Applicare una politica di aggiornamento e gestione della configurazione.** Introdurre controlli regolari per verificare che le configurazioni rispettino le best practice di sicurezza e che ogni nuova modifica sia validata in modo controllato.

5. Findings Summary

In questo capitolo vengono mostrati con dettaglio tutti i problemi di sicurezza identificati durante l'attività di penetration testing.

5.1 Descrizione delle vulnerabilità riscontrate

In tabella Tabella 5.1 sono mostrate le vulnerabilità identificate nell'asset.

CVE ID	Descrizione	CVE Score (CVSS 3.1)	Severità
CVE-2021-26691 [2]	Il modulo `mod_session` di Apache 2.40-2.4.46 contiene un bug critico che può causare crash o esecuzione di codice arbitrario, portando a un'escalation di privilegi o denial of service (DoS).	9.8	Critical
CVE-2018-14009 [3]	Il sistema espone pubblicamente l'IDE Codiad, il quale presenta una vulnerabilità nota di Remote Code Execution che consente l'esecuzione di comandi remoti senza autenticazione.	9.8	Critical
CVE-2019-0211 [4]	In Apache HTTP Server da 2.4.17 a 2.4.38, codice eseguito in thread secondari con privilegi minori può eseguire codice arbitrario con privilegi del processo principale (tipicamente root).	7.8	High
CVE-2019-0215 [5]	In Apache HTTP Server 2.4.37 e 2.4.38, un bug in `mod_ssl` può permettere a un client di eludere le restrizioni di accesso configurate per TLSv1.3, causando una violazione dei controlli.	7.5	High

CVE-2021-26690 [6]	Una vulnerabilità nel modulo `mod_session` di Apache HTTP Server 2.4.0–2.4.46, può portare al crash del server o a un denial of service (DoS) quando vengono gestite sessioni malformate.	7.5	High
CVE-2019-0217 [7]	Un problema di race condition nel modulo `mod_auth_digest` di Apache HTTP Server ≤ 2.4.38 consente di bypassare i meccanismi di autenticazione, permettendo accesso non autorizzato.	7.5	High
CVE-2020-35452 [8]	Il modulo `mod_auth_digest` di Apache HTTP Server 2.4.0–2.4.46 contiene un errore di overflow dello stack che può essere sfruttato per eseguire codice arbitrario o bloccare il server.	7.3	High
CVE-2023-51385 [9]	OpenSSH fino alla versione 9.3p1 (inclusa), in certe condizioni specifiche, permette l'esecuzione di comandi senza autorizzazione completa. Può essere sfruttato in contesti particolari per ottenere accesso non previsto.	6.5	Medium
CVE-2018-5164 [10]	Content Security Policy (CSP) non applicata correttamente in Firefox, consentendo l'esecuzione di script non autorizzati.	6.1	Medium
CVE-2023-48795 [11]	La vulnerabilità Terrapin in SSH, presente nelle versioni precedenti alla 9.6, consente la manipolazione della sequenza di pacchetti di avvio, riducendo la protezione del canale crittografato e potenzialmente compromettendo la sicurezza della connessione.	5.9	Medium

CVE-2003-1418 [12]	In Apache, l'intestazione ETag può rivelare dettagli sul filesystem, come l'inode del file, che possono essere usati per inferenze o attacchi di tipo file enumeration.	5.0	Medium
CVE-1999-0524 [13]	Il sistema risponde ai pacchetti ICMP Timestamp. Questo comportamento può consentire a un attaccante remoto di determinare l'orario del sistema e sincronizzare attacchi basati sul tempo.	2.1 (CVSS v2.0)	Low

Tabella 5.1: Vulnerabilità riscontrate

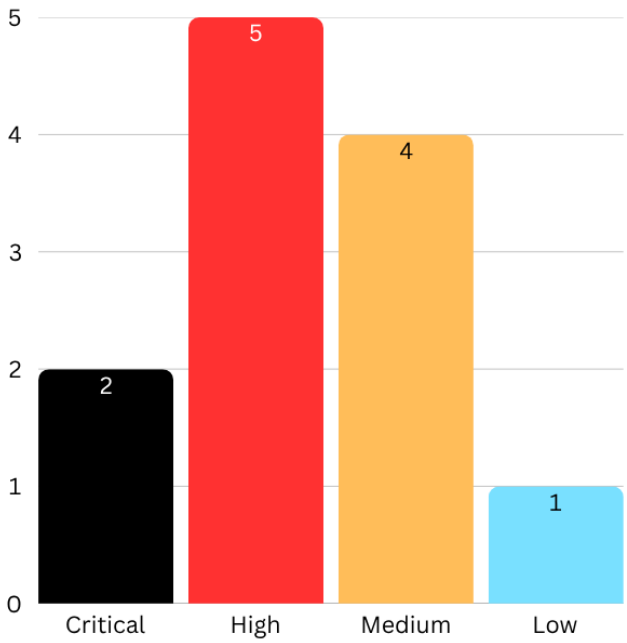

Figura 5.1: Grafico vulnerabilità per gravità

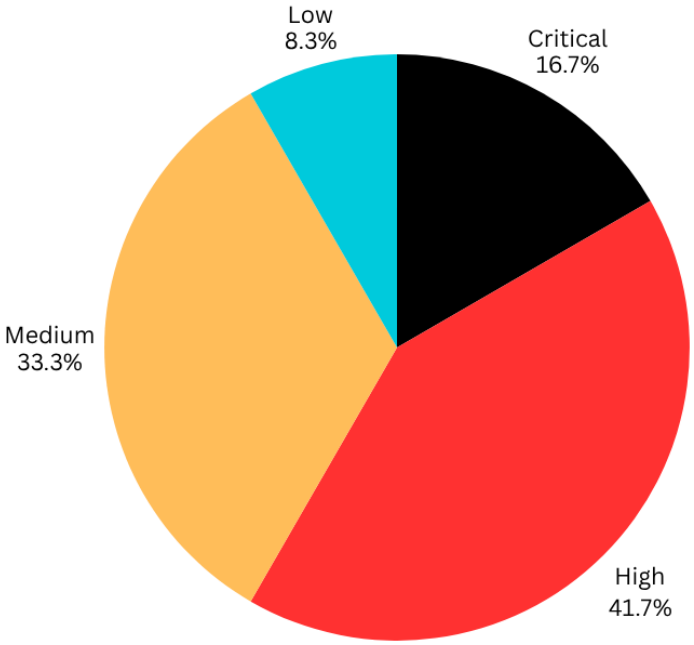

Figura 5.2: Grafico vulnerabilità per percentuale di gravità

5.2 Descrizione delle debolezze riscontrate

In tabella Tabella 5.2 vengono illustrate le debolezze identificate all'interno dell'asset.

CWE ID	Nome	Descrizione
CWE-1021 [14]	Improper Restriction of Rendered UI Layers or Frames	L'intestazione HTTP X-Frame-Options è assente, esponendo l'applicazione a vulnerabilità di tipo Clickjacking. Gli attaccanti potrebbero indurre un utente a interagire con contenuti malevoli mascherati da elementi dell'interfaccia.
CWE-521 [15]	Weak Password Requirements	L'autenticazione HTTP Basic accetta credenziali deboli, facilmente indovinabili tramite attacchi di forza bruta, esponendo l'ambiente Codiad ad accessi non autorizzati.
CWE-497 [16]	Exposure of System Data to an Unauthorized Control Sphere	L'intestazione Server nella risposta HTTP espone dettagli del software. Queste informazioni possono facilitare gli attaccanti nell'individuare vulnerabilità note associate alla versione specifica.
CWE-327 [17]	Use of a Broken or Risky Cryptographic Algorithm	l'uso di MAC deboli nel protocollo SSH espone la comunicazione a potenziali attacchi.
CWE-732 [18]	Incorrect Permission Assignment for Critical Resource	Permessi impropri assegnati al file /etc/sudoers, una risorsa critica, che ne consentono lettura e modifica non autorizzate.
CWE-256 [19]	Plaintext Storage of a Password	Presenza di file contenenti credenziali salvate in chiaro nel filesystem.

Tabella 5.2: Debolezze riscontrate

5.3 Valutazione dei rischi

Il presente capitolo illustra la valutazione dei rischi associati alle vulnerabilità identificate, attraverso la Hazard Risk Assessment Matrix (Tabella 5.3).

1. **CVE-2021-26691**: un overflow nell'heap può consentire l'esecuzione di codice arbitrario con privilegi di sistema, portando a compromissione totale del server. (1C)
2. **CVE-2018-14009** un'attaccante remoto può eseguire comandi a piacimento senza autenticazione, ottenendo il pieno controllo dell'applicazione e possibilmente dell'host sottostante. (1C)
3. **CVE-2019-0211**: un utente in grado di inviare richieste al server può ottenere privilegi di root, compromettendo l'intero sistema. (1E)
4. **CVE-2019-0215**: configurazioni TLSv1.3 errate possono permettere a un client di aggirare le restrizioni e accedere a risorse protette. (3D)
5. **CVE-2021-26690**: una condizione malformata nelle sessioni può bloccare o crashare il server, causando interruzione di servizio. (3B)
6. **CVE-2019-0217**: una concorrenza di richieste può far saltare l'autenticazione Digest, consentendo accessi non autorizzati. (2E)
7. **CVE-2020-35452**: un attaccante locale o remoto può mandare in crash il server tramite un overflow, interrompendo il servizio. (3C)
8. **CVE-2023-51385**: sfruttando opzioni come ProxyCommand, un attaccante può inserire e far eseguire comandi arbitrari sul server SSH. (2D)
9. **CVE-2018-5164:** esposizione a Cross-Site Scripting, permettendo l'iniezione di script malevoli per furto di cookie, hijacking di sessione e defacement (3C).
10. **CVE-2023-48795**: un attaccante MITM può manipolare i pacchetti di handshake, abbassando la sicurezza della cifratura e potenzialmente intercettando la sessione. (3D)
11. **CVE-2003-1418**: l'intestazione ETag rivela dettagli interni del filesystem che possono facilitare attacchi di fingerprinting o enumeration. (3D)
12. **CVE-1999-0524**: rispondendo a richieste timestamp, il sistema espone l'ora di sistema, agevolando attacchi sincronizzati o basati sul tempo. (4B)
13. **CWE-1021**: senza X-Frame-Options il sito è vulnerabile a clickjacking, con possibilità di indurre l'utente a compiere azioni involontarie. (3E)
14. **CWE-732**: Un utente locale può eseguire comandi con privilegi di root senza autenticazione, compromettendo completamente la sicurezza del sistema. (2C)

15. **CWE-521:** L'utilizzo di credenziali deboli nell'autenticazione HTTP espone il sistema a facili attacchi di forza bruta e accessi non autorizzati. (3C)
16. **CWE-497**: l'intestazione rivela la versione del software, facilitando la ricerca di exploit noti per quella release. (4E)
17. **CWE-327**: Utilizzo di MAC deboli in SSH può compromettere l'integrità dei dati trasmessi, esponendo la sessione a manipolazioni o attacchi crittografici. (3C)
18. **CWE-256** file leggibili contengono password in testo, che un utente con accesso limitato può leggere e riutilizzare per ottenere ulteriori privilegi. (1B)

Rischio / Occorrenza	1-Catastrofico	2 - Critico	3 - Serio	4-Minore
A – Frequente	0	0	1	0
B – Probabile	1	0	1	1
C – Occasionale	2	1	4	0
D – Remoto	0	1	2	0
E - Improbabile	1	1	1	1

Tabella 5.3: Hazard Risk Assessment Matrix

6 Detailed Summary

Di seguito sono presentate le schede relative alle principali criticità riscontrate nell'asset analizzato. La suddivisione in sezioni tiene conto del livello di gravità assegnato secondo la metrica CVSS 3.1 per le vulnerabilità individuate, e dell'impatto stimato per le debolezze di configurazione sulla base delle segnalazioni fornite dagli strumenti di analisi utilizzati.

6.1 Operating System (OS) End of Life (EOL) Detection

Titolo:	Operating System (OS) End of Life (EOL) Detection	**CVE**
	10.0 Critico	-
Descrizione:		
Il sistema operativo installato sul target (Debian GNU/Linux 10) ha raggiunto la fine del ciclo di supporto (EOL) il 30/06/2024. Ciò significa che non riceve più aggiornamenti di sicurezza dal fornitore, esponendo l'host a numerose vulnerabilità note e future.		
Impatto:		
L'assenza di aggiornamenti rende il sistema facilmente attaccabile attraverso vulnerabilità non mitigate, potenzialmente già note pubblicamente. L'host può quindi essere compromesso anche senza vulnerabilità zero-day.		
Soluzione:		
Aggiornare il sistema operativo a una versione attivamente supportata.		
Metodo di detection:		
OpenVAS		

6.2 Heap Overflow in Apache HTTP Server

Titolo:	Heap Overflow in Apache HHTP Server	**CVE**
	9.8 Critico	2021-26691
Descrizione:		
Nelle versioni di Apache HTTP Server dalla 2.4.0 alla 2.4.46, un SessionHeader appositamente creato inviato da un server di origine potrebbe causare un overflow dell'heap.		
Impatto:		
Un attaccante remoto non autenticato, controllando un server back-end o proxy, potrebbe inviare il SessionHeader malformato e provocare un crash del servizio (Denial of Service) o, in scenari più avanzati, arrivare a eseguire codice arbitrario con i privilegi del processo HTTPd.		
Soluzione:		
Aggiornare Apache HTTP Server alla versione 2.4.47 o successiva, in cui il problema è stato corretto.		
Metodo di detection:		
Analisi manuale		

6.3 Esecuzione di codice remoto in Codiad

Titolo:	Esecuzione di codice remoto in Codiad	**CVE**
	9.8 Critico	2018-14009
Descrizione:		
Nelle versioni di Codiad fino alla 2.8.4, un input non correttamente validato consente a un attaccante remoto di iniettare e eseguire comandi arbitrari sul server che ospita l'applicazione.		
Impatto:		
Un attaccante remoto può eseguire codice arbitrario con i privilegi del processo web.		
Soluzione:		
Aggiornare Codiad ad una versione non vulnerabile oppure limitare l'accesso all'interfaccia di Codiad tramite firewall o VPN, esponendo il servizio solo a reti fidate.		
Metodo di detection:		
Analisi manuale		

6.4 Weak Password Requirements

Titolo:	Weak Password Requirements	**CWE**
	Critico	521
Descrizione:		
I meccanismi di autenticazione si basano spesso su un segreto memorizzato (noto anche come password) per fornire un'asserzione di identità all'utente di un sistema. È quindi importante che questa password sia sufficientemente complessa e difficile da indovinare per un avversario. I requisiti specifici relativi alla complessità di una password dipendono dal tipo di sistema da proteggere. La selezione dei requisiti di password corretti e la loro applicazione durante l'implementazione sono fondamentali per il successo complessivo del meccanismo di autenticazione.		
Impatto:		
L'utilizzo di password deboli aumenta significativamente il rischio di accessi non autorizzati, in quanto un attaccante può sfruttare tecniche di brute-force o dizionario per compromettere account legittimi e accedere a risorse sensibili del sistema.		
Soluzione:		
Introdurre requisiti minimi di complessità per le password (lunghezza minima e massima, limitazione al riutilizzo delle password, limitazioni all'uso di password comuni, uso di caratteri speciali) e sostituire le credenziali deboli.		
Metodo di detection:		
Analisi manuale		

6.5 Plaintext Storage of a Password

Titolo:	Plaintext Storage of a Password	**CWE**
	-	256
Descrizione:		
I problemi di gestione delle password si verificano quando una password viene memorizzata in chiaro nelle proprietà, nel file di configurazione o nella memoria di un'applicazione.		
Impatto:		
Memorizzare una password in chiaro in un file di configurazione consente a chiunque possa leggere il file di accedere alla risorsa protetta da password. In alcuni contesti, anche la memorizzazione di una password in chiaro in memoria è considerata un rischio per la sicurezza se la password non viene cancellata immediatamente dopo il suo utilizzo.		
Soluzione:		
Evitare di conservare le password in luoghi facilmente accessibili.		
Metodo di detection:		
Analisi manuale		

6.6 Incorrect Permission Assignment for Critical Resource

Titolo:	Incorrect Permission Assignment for Critical Resource	**CWE**
	-	732
Descrizione:		
Il prodotto specifica le autorizzazioni per una risorsa critica per la sicurezza in modo tale da consentire la lettura o la modifica di tale risorsa da parte di soggetti non autorizzati. In particolare, nel file /etc/sudoers è stata concessa all'utente non-root l'opzione NOPASSWD su uno o più comandi, permettendo l'esecuzione di operazioni elevate senza alcuna autenticazione.		
Impatto:		
L'utente può acquisire privilegi di root senza bisogno di inserire la propria password, bypassando completamente i controlli di sicurezza e potendo eseguire qualunque azione sul sistema.		
Soluzione:		
Rimuovere l'opzione NOPASSWD e richiedere sempre l'inserimento della password per i comandi sudo.		
Metodo di detection:		
Analisi manuale		

6.7 Apache HTTP Server command injection

Titolo:	Apache HTTP Server command injection	**CVE**
	7.8 Alto	CVE-2019-0211
Descrizione:		
Nelle versioni 2.4 di Apache HTTP Server (dalla 2.4.17 alla 2.4.38), con evento MPM, worker o prefork, il codice in esecuzione in processi o thread figlio con privilegi inferiori (inclusi gli script eseguiti da un interprete di scripting in-process) poteva eseguire codice arbitrario con i privilegi del processo padre (solitamente root) manipolando la scoreboard. I sistemi non Unix non sono interessati.		
Impatto:		
Un attaccante che riesca a iniettare codice in uno script lato server può elevarne i privilegi fino a root, compromettendo l'intero sistema web.		
Soluzione:		
Aggiornare ad Apache ≥ 2.4.39		
Metodo di detection:		
Analisi manuale		

6.8 Bypass del controllo accessi client in mod_ssl (TLS 1.3)

Titolo:	Bypass del controllo accessi client in mod_ssl (TLS 1.3)	**CVE**
	7.5 Alto	2019-0215
Descrizione:		
Nelle versioni 2.4.37 e 2.4.38 di Apache HTTP Server, un bug in mod_ssl, quando si utilizzava la verifica del certificato client per posizione con TLSv1.3, consentiva a un client di aggirare le restrizioni di controllo degli accessi configurate.		
Impatto:		
Consente la lettura, modifica o cancellazione di dati riservati e può provocare denial of service. Un attaccante remoto con accesso di base al servizio web può consultare o manipolare risorse altrimenti riservate a client autenticati.		
Soluzione:		
Installare Apache HTTP Server 2.4.39 o successivo, dove il problema è stato risolto.		
Metodo di detection:		
Analisi manuale		

6.9 Denial of Service in mod_session via NULL pointer dereference

Titolo:	Denial of Service in mod_session via NULL pointer dereference	**CVE**
	7.5 Alto	2021-26690
Descrizione:		
Versioni di Apache HTTP Server da 2.4.0 a 2.4.46 un'intestazione Cookie appositamente creata e gestita da mod_session può causare la dereferenziazione del puntatore NULL e l'arresto anomalo, portando a un possibile Denial Of Service.		
Impatto:		
Un attacker remoto può inviare un singolo Cookie malformato per far crashare Apache HTTPd, causando un Denial of Service completo del server web.		
Soluzione:		
passare ad Apache HTTP Server **2.4.47** o successivo, dove il problema è stato corretto.		
Metodo di detection:		
Analisi manuale		

6.10 Bypass di autenticazione in mod_auth_digest

Titolo:	Bypass di autenticazione in mod_auth_digest	CVE
	7.5 Alto	2019-0217
Descrizione:		
In Apache HTTP Server versione 2.4.38 e precedenti, una race condition in mod_auth_digest, se eseguita in un server con thread, poteva consentire a un utente con credenziali valide di autenticarsi utilizzando un altro nome utente, aggirando le restrizioni di controllo degli accessi configurate.		
Impatto:		
Un utente autenticato può impersonare un altro account, accedendo a risorse non autorizzate e compromettendo la confidenzialità e l'integrità dei dati sul server.		
Soluzione:		
Aggiornare Apache HTTP Server a 2.4.39 o successivo, dove la race è stata corretta.		
Metodo di detection:		
Analisi manuale		

6.11 Stack overflow in mod_auth_digest tramite nonce malformato

Titolo:	Stack overflow in mod_auth_digest tramite nonce malformato	**CVE**
	7.3 Alto	2020-35452
Descrizione:		
Nelle versioni di Apache HTTP Server dalla 2.4.0 alla 2.4.46, un Digest-nonce appositamente costruito può innescare un overflow di stack in mod_auth_digest, dovuto al fatto che viene processato senza un'adeguata validazione delle dimensioni. Pur non essendoci al momento exploit noti, alcune combinazioni di compilatore e opzioni potrebbero renderlo sfruttabile, benché l'overflow riguardi un solo byte di valore zero.		
Impatto:		
Un attaccante remoto, senza alcun privilegio e senza interazione utente, può inviare un nonce malformato per corrompere lo stack del processo HTTPd, con possibili crash o corruzione di memoria che impattano lievemente confidenzialità, integrità e disponibilità del servizio.		
Soluzione:		
Aggiornare Apache HTTP Server a 2.4.47 o successivo, dove la validazione del Digest nonce è stata rafforzata.		
Metodo di detection:		
Analisi manuale		

6.12 Iniezione di comandi OS in OpenSSH tramite expansion token

Titolo:	Iniezione di comandi OS in OpenSSH tramite expansion token	**CVE**
	6.5 Medio	2023-51385
Descrizione:		
In ssh, in OpenSSH prima della versione 9.6, l'iniezione di comandi del sistema operativo poteva verificarsi se un nome utente o un nome host conteneva metacaratteri shell e, in determinate situazioni, questo nome veniva referenziato da un token di espansione. Ad esempio, un repository Git non attendibile può avere un sottomodulo con metacaratteri shell in un nome utente o in un nome host.		
Impatto:		
Un repository Git malevolo o una configurazione SSH che sfrutti token di espansione con nomi non sanitizzati può indurre il client OpenSSH ad eseguire comandi a insaputa dell'utente, compromettendo confidenzialità e integrità dei dati sul sistema locale.		
Soluzione:		
Aggiorna OpenSSH alla versione 9.6 o successiva, dove la sanitizzazione degli expansion token è stata corretta.		
Metodo di detection:		
Analisi manuale		

6.13 Content Security Policy (CSP) Header Not Set

Titolo:	Protection Mechanism Failure Content Security Policy (CSP) Header Not Set	**CVE**
	6.1 Medio	2018-5164
Descrizione:		
Content Security Policy (CSP) è un livello di sicurezza aggiuntivo che aiuta a rilevare e mitigare determinati tipi di attacchi, inclusi Cross-Site Scripting (XSS) e attacchi di iniezione di dati. Questi attacchi vengono utilizzati per tutto, dal furto di dati alla manomissione del sito o alla distribuzione di malware. CSP fornisce una serie di header HTTP standard che consentono ai gestori del sito di dichiarare le fonti di contenuto approvate che i browser sono autorizzati a caricare su quella pagina — i tipi coperti includono JavaScript, CSS, frame HTML, font, immagini e oggetti incorporabili come applet Java, ActiveX, file audio e video.		
Impatto:		
Senza una Content-Security-Policy, il sito rimane vulnerabile a Cross-Site Scripting, iniezioni di contenuto e relative compromissioni di dati, defacement o distribuzione di malware.		
Soluzione:		
Assicurarsi che il server web, application server, load balancer, ecc. siano configurati per impostare l'header Content-Security-Policy.		
Metodo di detection:		
OWASP ZAP		

6.14 Terrapin attack

Titolo:	Terrapin attack	**CVE**
	5.9 Medio	2023-48795
Descrizione:		
Il protocollo SSH con alcune estensioni OpenSSH, presenti in OpenSSH prima della versione 9.6 e in numerose altre implementazioni, consente ad aggressori remoti di bypassare i controlli di integrità in modo che alcuni pacchetti vengano omessi durante la negoziazione delle estensioni (alias "Terrapin" attack). Ciò avviene perché il Binary Packet Protocol (BPP) di SSH, implementato da queste estensioni, gestisce in modo errato la fase di handshake e l'utilizzo dei numeri di sequenza, permettendo di declassare o disabilitare alcune funzionalità di sicurezza (ad es. ChaCha20-Poly1305 e gli algoritmi MAC Encrypt-then-MAC).		
Impatto:		
Un aggressore in rete può forzare la negoziazione di algoritmi meno sicuri o disabilitare controlli di integrità, mettendo a rischio confidenzialità e integrità del canale SSH.		
Soluzione:		
Aggiornare OpenSSH alla 9.6 (o successiva).		
Metodo di detection:		
Nessus		

6.15 Disclosure di informazioni in Apache HTTP Server

Titolo:	Disclosure di informazioni in Apache HTTP Server	**CVE**
	4.3 Medio	2003-1418
Descrizione:		
Nelle versioni di Apache HTTP Server 1.3.22 fino alla 1.3.27 su OpenBSD, il server inserisce nell'header ETag il numero di inode dei file e utilizza boundary multipart MIME che espongono i PID dei processi child. Un attaccante remoto può leggere questi valori semplicemente analizzando le risposte HTTP.		
Impatto:		
Un avversario remoto ottiene dati di sistema (inode e PID) utili per fingerprinting del filesystem e del processo, facilitando la ricognizione e la preparazione di attacchi successivi.		
Soluzione:		
Aggiornare Apache HTTP Server alla versione 1.3.28 o successiva, in cui il problema è stato risolto.		
Metodo di detection:		
Nikto		

6.16 Missing Anti-clickjacking header

Titolo:	Improper Restriction of Rendered UI Layers or Frames	**CWE**
	-	1021
Descrizione:		
L'intestazione HTTP X-Frame-Options è assente, esponendo l'applicazione a clickjacking: un utente può essere indotto a interagire con elementi mascherati.		
Impatto:		
Possibilità di clickjacking, con utenti indotti a compiere azioni non desiderate.		
Soluzione:		
I moderni browser Web supportano le intestazioni HTTP Content-Security-Policy e X-Frame-Options. Assicurarsi che almeno una di queste sia impostata su tutte le pagine restituite dal sito/app. Se è preveisto che la pagina possa essere inserita in un frame solo da pagine dello stesso server (ad esempio perché fa parte di un FRAMESET), utilizzare SAMEORIGIN. Se invece non è mai aspettato mai la pagina venga inserita in un frame, usare DENY. In alternativa, valutare di implementare la direttiva frame-ancestors di Content Security Policy.		
Metodo di detection:		
OWASP ZAP/Nikto		

6.17 Weak MAC Algorithm(s) Supported (SSH)

Titolo:	Weak MAC Algorithm(s) Supported (SSH)	**CWE**
	2.6 Bassa*	327
Descrizione:		
Il server SSH remoto è configurato per supportare algoritmi MAC deboli, come umac-64-etm@openssh.com e umac-64@openssh.com. Questi algoritmi non garantiscono adeguati livelli di sicurezza crittografica e potrebbero consentire a un attaccante di manipolare i dati in transito o indebolire la protezione della sessione.		
Impatto:		
L'uso di MAC deboli può compromettere l'integrità dei dati trasmessi durante la sessione SSH, rendendo possibile l'alterazione dei messaggi o la degradazione della sicurezza della comunicazione.		
Soluzione:		
Modificare la configurazione di SSH (/etc/ssh/sshd_config) per disabilitare gli algoritmi MAC deboli.		
Metodo di detection:		
OpenVAS		

*CVSS versione 2.0

6.18 ICMP Timestamp Request Remote Date Disclosure

Titolo:	ICMP Timestamp Request Remote Date Disclosure	**CVE**
	2.1 Bassa*	1999-0524
Descrizione:		
Le informazioni ICMP quali (1) netmask e (2) timestamp sono consentite da host arbitrari.		
Impatto:		
Un aggressore remoto può raccogliere informazioni sulla topologia della rete (netmask) e sullo skew temporale del sistema (timestamp), facilitando la ricognizione, il fingerprinting del sistema operativo e la pianificazione di attacchi successivi.		
Soluzione:		
Disabilitare le risposte ICMP di tipo Timestamp e Address Mask a livello di firewall.		
Metodo di detection:		
Nessus/OpenVAS		

*CVSS versione 2.0

6.19 Server Leaks Version Information via "Server" HTTP Response Header Field

Titolo:	Exposure of Sensitive System Information to an Unauthorized Control Sphere	**CWE**
	-	497
Descrizione:		
Il server web/applicazione sta divulgando informazioni sulla versione tramite l'intestazione di risposta HTTP Server.		
Impatto:		
L'accesso a tali informazioni può agevolare un attaccante nell'individuazione di altre vulnerabilità a cui il vostro server web/applicazione è soggetto.		
Soluzione:		
Assicurarsi che il server web, il server applicativo, il bilanciatore di carico, ecc. siano configurati per sopprimere l'intestazione **Server** oppure per restituire informazioni generiche.		
Metodo di detection:		
OWASP ZAP		

6.20 X-Content-Type-Options Header Missing

Titolo:	X- Content-Type-Options Header Missing	**CWE**
	-	-
Descrizione:		
L'header anti-MIME-sniffing X-Content-Type-Options non è stato impostato su 'nosniff'.		
Impatto:		
Ciò permette alle versioni più datate di Internet Explorer e Chrome di eseguire il MIME-sniffing sul corpo della risposta, potenzialmente interpretando e mostrando il contenuto con un tipo diverso da quello dichiarato. Le versioni correnti (inizio 2014) e legacy di Firefox, invece, utilizzeranno il tipo di contenuto dichiarato (se presente) anziché fare MIME-sniffing, ma in assenza di un header "nosniff" rimane il rischio per i client vulnerabili.		
Soluzione:		
Verificare che il server applicativo/web imposti correttamente l'intestazione Content-Type e Assicurarsi che su tutte le pagine web venga inviato l'header X-Content-Type-Options: nosniff. Se possibile, utilizzare browser moderni e conformi agli standard, privi di MIME-sniffing automatico o configurabili tramite il server per disabilitare tale comportamento.		
Metodo di detection:		
OWASP ZAP/Nikto		

7 References

[1] Vulnerable by Design, «Inferno 1.1,» [Online]. Available: https://www.vulnhub.com/?q=inferno.

[2] National Institute of Standards and Technology, «CVE-2021-26691 Detail,» NVD – U.S. Department of Commerce, 2021. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2021-26691.

[3] National Institute of Standards and Technology, «CVE-2018-14009 Detail,» NVD – U.S. Department of Commerce, 2018. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2018-14009.

[4] National Institute of Standards and Technology, «CVE-2019-0211 Detail,» NVD – U.S. Department of Commerce, 2019. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-0211.

[5] National Institute of Standards and Technology, «CVE-2019-0215 Detail,» NVD – U.S. Department of Commerce, 2019. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-0215.

[6] National Institute of Standards and Technology, «CVE-2021-26690 Detail,» NVD – U.S. Department of Commerce, 2021. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2021-26690.

[7] National Institute of Standards and Technology, «CVE-2019-0217 Detail,» NVD – U.S. Department of Commerce, 2019. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2019-0217.

[8] National Institute of Standards and Technology, «CVE-2020-35452 Detail,» NVD – U.S. Department of Commerce, 2020. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2020-35452.

[9] National Institute of Standards and Technology, «CVE-2023-51385 Detail,» NVD – U.S. Department of Commerce, 2023. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2023-51385.

[10] National Institute of Standards and Technology, «CVE-2018-5164 Detail,» NVD – U.S. Department of Commerce, 2018. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2018-5164.

[11] National Institute of Standards and Technology, «CVE-2023-48795 Detail,» NVD – U.S. Department of Commerce, 2023. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2023-48795.

[12] National Institute of Standards and Technology, «CVE-2003-1418 Detail,» NVD – U.S. Department of Commerce, 2003. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-2003-1418.

[13] National Institute of Standards and Technology, «CVE-1999-0524 Detail,» NVD – U.S. Department of Commerce, 1999. [Online]. Available: https://nvd.nist.gov/vuln/detail/cve-1999-0524.

[14] MITRE Corporation, «CWE-1021: Improper Restriction of Rendered UI Layers or Frames,» MITRE, 2017. [Online]. Available: https://cwe.mitre.org/data/definitions/1021.html.

[15] MITRE Corporation, «CWE-521: Weak Password Requirements,» MITRE, 2006. [Online]. Available: https://cwe.mitre.org/data/definitions/521.html.

[16] MITRE Corporation, «CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere,» MITRE, 2006. [Online]. Available: https://cwe.mitre.org/data/definitions/497.html.

[17] MITRE Corporation, «CWE-327: Use of a Broken or Risky Cryptographic Algorithm,» MITRE, 2006. [Online]. Available: https://cwe.mitre.org/data/definitions/327.html.

[18] MITRE Corporation, «CWE-732: Incorrect Permission Assignment for Critical Resource,» MITRE, 2008. [Online]. Available: https://cwe.mitre.org/data/definitions/732.html.

[19] MITRE Corporation, «CWE-256: Plaintext Storage of a Password,» MITRE, [Online]. Available: https://cwe.mitre.org/data/definitions/256.html.

8 Appendix

Tutti i risultati delle scansioni effettuate con gli strumenti di analisi, gli script utilizzati per lo sfruttamento delle vulnerabilità individuate e il documento contenente il processo completo di penetration testing (**Documento di replicabilità**) sono disponibili in un repository GitHub dedicato, accessibile al seguente indirizzo: https://github.com/MarioLezzi92/Inferno-1.1