UNIVERSITÀ DEGLI STUDI DI SALERNO

Dipartimento di Informatica

Corso di Laurea Magistrale in Informatica

CORSO DI PENETRATION TESTING
AND ETHICAL HACKING

Cengbox: 1: Penetration Testing Report

STUDENTE

Mattia d'Argenio

Matricola: 0522501524

DOCENTE

Prof. **Arcangelo Castiglione**

Università degli studi di Salerno

Anno Accademico 2023-2024

Indice

CAPITOLO 1

Penetration Testing Report

1.1 Executive Summary

Al fine di realizzare il progetto del corso *Penetration Testing and Ethical Hacking* sono state svolte delle attività di Penetration Testing su una macchina virtuale vulnerabile chiamata **Cengbox: 1**. Il fine ultimo di tutte le attività svolte è stato semplicemente didattico, con lo scopo di acquisire al meglio tutte le conoscenze fornite durante lo svolgimento del corso. Per l'esecuzione di tutte le attività è stata adottata una strategia di analisi *Black-Box*, quindi senza avere nessuna conoscenza pregressa sull'asset, e sono state realizzate all'interno di un'ambiente simulato con una connessione diretta con l'asset.
Durante le varie attività svolte sono state riscontrate diverse vulnerabilità che possono portare un malintenzionato ad ottenere documenti o file a cui non dovrebbe avere accesso e, nel caso peggiore, alla compromissione totale del sistema.

1.2 Engagement Highlights

Dal momento che il processo di Penetration Testing è stato svolto in un contesto puramente didattico, non è stato necessario definire particolari regole di ingaggio.

1.3 Vulnerability Report

Durante il processo sono state trovate varie vulnerabilità, la maggior parte con gravità **media**, alcune con gravità **bassa**. Le principali sono le seguenti:

- *Information Leakage* (gravità **media**): alcune informazioni importanti sono salvate in maniera non protetta fornendo ad un attaccante la possibilità di compromettere le password degli utenti e dell'amministratore;
- Navigabilità delle **directory** del Web Server (gravità **media**): le directory del Web Server mediante il Web Browser al fine di visualizzarne il contenuto;
- Utilizzo di una versione deprecata di **jQuery** (gravità **media**): Viene utilizzata una versione della libreria **jQuery** che è vulnerabile ad un attacco che permette ad un attaccante di rubare informazioni sensibili ai client che visitano una pagina con integrata quella libreria;
- Supportati protocolli deboli per *SSH* (gravità **bassa**): per le connessioni *SSH* è abilitato il supporto a protocolli di scambio di chiavi e di autenticazione che sono deboli e facilmente attaccabili;
- Trapelamento dei **timestamp** del sistema (gravità **bassa**):] ottenimento di informazioni sul timestamp del sistema con eventuale possibilità di prevedere dati generati in maniera arbitraria dal sistema

1.4 Remediation Report

Durante il processo eseguito, sono state trovate molte vulnerabilità tra cui alcune abbastanza importanti che potrebbero comportare la compromissione completa del sistema e di file e documenti all'interno, nonchè la compromissione dei dati dei visitatori del sito web. Per questa ragione, si forniscono i seguenti consigli per migliorare la sicurezza dell'asset:

- Rimuovere le informazioni sensibili non correttamente protette;
- Riconfigurazione del **Web Server** al fine di impedire la navigazione delle directory e di impostare opportuni attributi di sicurezza;
- Aggiornare la versione di **jQuery** utilizzata nelle pagine web;
- Inibizione del trapelamento delle informazioni relative al **timestamp** del sistema;

- Configurare il servizio *SSH* in modo tale che non supporti protocolli crittografici deboli;

1.5 Findings Summary

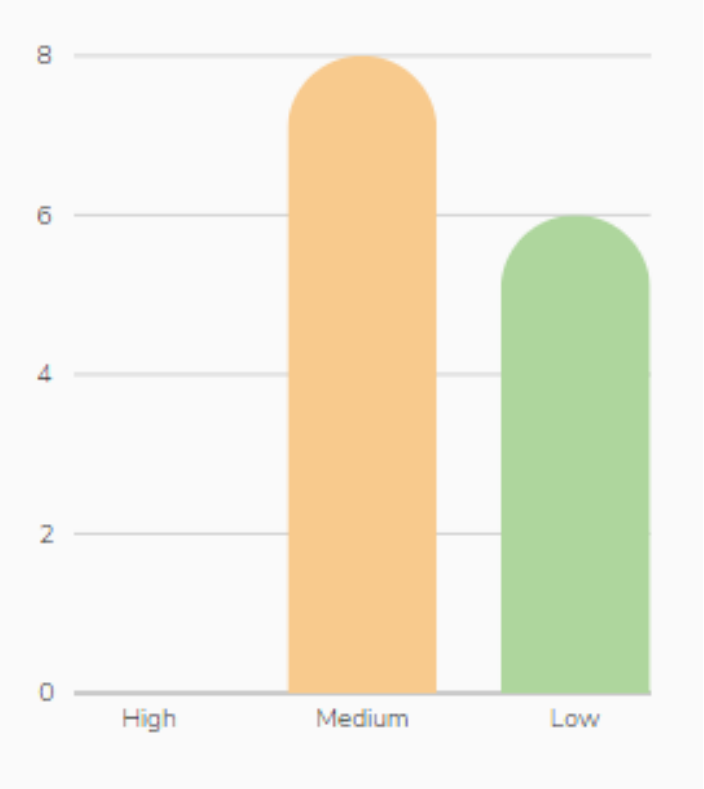

Figura 1.1: Ortogramma riassuntivo dei rilevamenti

1.6 Detailed Summary

Di seguito saranno elencate le varie vulnerabilità riscontrate e saranno indicati i documenti esaustivi nei quali consultare tutte le restanti vulnerabilità riscontrate grazie a tool di rilevazione automatica.

1.6.1 Vulnerabilità rilevate mediante i tool

Rilevamenti effettuati da *Nessus*

Con il tool *Nessus* sono stati generati due report, entrambi posti nella cartella *Report* e con il nome **nessus_vuln_scan.pdf** e **nessus_vuln_scan_web.pdf**.

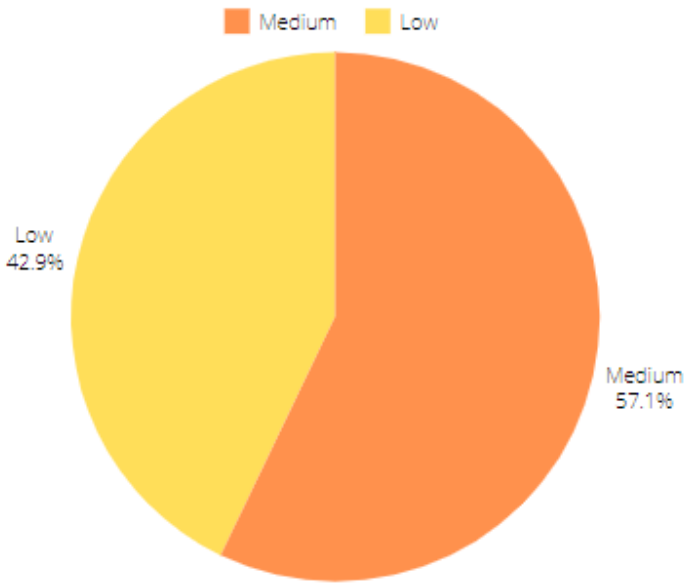

Figura 1.2: Aerogramma riassuntivo dei rilevamenti

Rilevamenti effettuati da *OpenVAS*

Con il tool *OpenVAS* è stato generato un solo report, posto nella cartella *Report* e con il nome **report-openvas.pdf**.

Rilevamenti effettuati da *OWASP ZAP*

Con il tool *OWASP ZAP* è stato generato un solo report, posto nella cartella *Report* e con il nome **report_finale.pdf**.

Rilevamenti effettuati da *Nikto*

Con il tool *Nikto* è stato generato un solo report, posto nella cartella *Report* e con il nome **report-nikto2.html**.

Titolo:	JQuery 1.2 < 3.5.0 Multiple XSS	**CVE**
	MEDIA	**2020-11022/11023**
Descrizione:		
La versione di JQuery ospitata sul server web remoto è vulnerabile a molteplici vulnerabilità di cross-site scripting (XSS).		
Impatto:		
Un utente malintenzionato può sfruttare tali vulnerabilità per eseguire script dannosi nel contesto di sicurezza del browser della vittima.		
Soluzione:		
Aggiornare JQuery alla versione 3.5.0 o successiva.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	SSH Terrapin Prefix Truncation Weakness	**CVE**
	MEDIA	**2023-48795**
Descrizione:		
Il server SSH remoto è vulnerabile a un attacco di troncazione del prefisso man-in-the-middle, che può consentire a un attaccante di bypassare i controlli di integrità e degradare la sicurezza della connessione.		
Impatto:		
Un utente malintenzionato può sfruttare tale vulnerabilità per intercettare o modificare il contenuto della connessione SSH.		
Soluzione:		
Aggiornare il server SSH e configurare protocolli di sicurezza più robusti.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	ICMP Timestamp Request Remote Date Disclosure	**CVE/CWE**
	MEDIA	**1999-0524/200**
Descrizione:		
La macchina target ha risposto ad una richiesta ICMP di timestamp. Tale informazione potrebbe essere sfruttata per violare servizi presenti sulla macchina target.		
Impatto:		
Un utente malintenzionato potrebbe utilizzare le informazioni di timestamp per condurre attacchi basati sul tempo.		
Soluzione:		
Disabilitare le risposte ICMP Timestamp sul sistema.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nessus.		

Titolo:	Weak MAC Algorithm(s) Supported (SSH)	**CVE**
	BASSA	**N/A**
Descrizione:		
Il server SSH remoto è configurato per supportare algoritmi MAC deboli.		
Impatto:		
Un attaccante può sfruttare questi algoritmi deboli per compromettere la confidenzialità e l'integrità della connessione SSH.		
Soluzione:		
Configurare il server SSH per supportare solo algoritmi MAC forti.		
Metodo di detection:		
Vulnerabilità individuata tramite il software OpenVAS.		

Titolo:	TCP Timestamps Information Disclosure	**CVE**
	BASSA	**N/A**
Descrizione:		
L'host remoto implementa i timestamp TCP, permettendo di calcolare il tempo di uptime.		
Impatto:		
Un attaccante può utilizzare queste informazioni per condurre attacchi di ricostruzione temporale.		
Soluzione:		
Disabilitare i timestamp TCP nel sistema.		
Metodo di detection:		
Vulnerabilità individuata tramite il software OpenVAS.		

Titolo:	Absence of Anti-CSRF Tokens	**CWE**
	MEDIA	**352**
Descrizione:		
Non sono stati trovati token Anti-CSRF in un modulo di invio HTML.		
Impatto:		
Gli attacchi CSRF (Cross-Site Request Forgery) possono forzare una vittima a inviare una richiesta HTTP a una destinazione senza la sua conoscenza o intento.		
Soluzione:		
Implementare token Anti-CSRF nei moduli HTML.		
Metodo di detection:		
Vulnerabilità individuata tramite il software OWASP ZAP.		

Titolo:	Content Security Policy (CSP) Header Not Set	**CWE**
	MEDIA	**693**
Descrizione:		
La politica di sicurezza dei contenuti (CSP) aiuta a rilevare e mitigare determinati tipi di attacchi come Cross-Site Scripting (XSS) e iniezione di dati. CSP fornisce un set di intestazioni HTTP standard che permettono ai proprietari di dichiarare le fonti approvate di contenuti che i browser dovrebbero caricare.		
Impatto:		
L'assenza di CSP espone il sito a vari tipi di attacchi.		
Soluzione:		
Configurare le intestazioni CSP nelle risposte HTTP.		
Metodo di detection:		
Vulnerabilità individuata tramite il software OWASP ZAP.		

Titolo:	Missing Anti-clickjacking Header	**CWE**
	MEDIA	**1021**
Descrizione:		
La risposta non include né la direttiva 'frame-ancestors' di Content-Security-Policy né X-Frame-Options per proteggere contro attacchi di tipo ClickJacking.		
Impatto:		
Il sito può essere vulnerabile a attacchi di clickjacking.		
Soluzione:		
Implementare le intestazioni di sicurezza X-Frame-Options o frame-ancestors nelle risposte HTTP.		
Metodo di detection:		
Vulnerabilità individuata tramite il software OWASP ZAP.		

Titolo:	Vulnerable JS Library	**CVE/CWE**
	MEDIA	**2020-11023/11022/829**
Descrizione:		
È stata identificata una libreria vulnerabile: jquery, versione 3.4.1.		
Impatto:		
Un attaccante può sfruttare le vulnerabilità della libreria per eseguire codice dannoso.		
Soluzione:		
Aggiornare la libreria JQuery alla versione più recente.		
Metodo di detection:		
Vulnerabilità individuata tramite il software OWASP ZAP.		

Titolo:	X-Content-Type-Options Header Missing	**CWE**
	BASSA	**693**
Descrizione:		
L'intestazione Anti-MIME-Sniffing X-Content-Type-Options non è impostata su 'nosniff', permettendo a versioni più vecchie di Internet Explorer e Chrome di eseguire il MIME-sniffing sul corpo della risposta.		
Impatto:		
Questo può permettere attacchi basati sull'interpretazione errata del tipo di contenuto.		
Soluzione:		
Configurare l'intestazione X-Content-Type-Options su 'nosniff' nelle risposte HTTP.		
Metodo di detection:		
Vulnerabilità individuata tramite il software OWASP ZAP.		

Titolo:	The anti-clickjacking X-Frame-Options header is not present	**CVE**
	MEDIA	**N/A**
Descrizione:		
L'header X-Frame-Options per prevenire il clickjacking non è presente.		
Impatto:		
Il sito è vulnerabile a attacchi di clickjacking.		
Soluzione:		
Implementare l'header X-Frame-Options nelle risposte HTTP.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nikto.		

Titolo:	The X-Content-Type-Options header is not set	**CVE**
	BASSA	**N/A**
Descrizione:		
L'intestazione Anti-MIME-Sniffing X-Content-Type-Options non è impostata su 'nosniff', permettendo a versioni più vecchie di Internet Explorer e Chrome di eseguire il MIME-sniffing sul corpo della risposta.		
Impatto:		
Questo può permettere attacchi basati sull'interpretazione errata del tipo di contenuto.		
Soluzione:		
Configurare l'intestazione X-Content-Type-Options su 'nosniff' nelle risposte HTTP.		
Metodo di detection:		
Vulnerabilità individuata tramite il software Nikto.		

Bibliografia

Siti Web consultati

- CWE-693 – https://cwe.mitre.org/data/definitions/693.html
- CWE-829 – https://cwe.mitre.org/data/definitions/829.html
- CWE-1021 – https://cwe.mitre.org/data/definitions/1021.html
- CWE-352 – https://cwe.mitre.org/data/definitions/352.html
- CVE-1999-0524 – https://nvd.nist.gov/vuln/detail/CVE-1999-0524
- CVE-2020-11022– https://nvd.nist.gov/vuln/detail/CVE-2020-11022
- CVE-2020-11023– https://nvd.nist.gov/vuln/detail/CVE-2020-11023
- CVE-2023-48795– https://nvd.nist.gov/vuln/detail/CVE-2023-48795