UNIVERSITÀ DEGLI STUDI DI SALERNO

Penetration Testing Report

CORROSION: 2

Federico De Mattia — Corso di PTEH — A.A. 2022/2023

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Indice

1 Executive Summary **2**

2 Engagement Highlights **2**

3 Vulnerability Report **2**

4 Remediation Report **2**

5 Findings Summary **3**

6 Detailed Summary **3**
6.1 High 3
6.2 Medium 5
6.3 Low 6
6.4 Informative 6

1 Executive Summary

Nel contesto del corso di Penetration Testing & Ethical Hacking, ho svolto un progetto che prevede l'esecuzione di un penetration test sulla macchina target denominata **Corrosion: 2**. L'obiettivo di questa attività è analizzare la sicurezza della macchina target e individuare eventuali vulnerabilità, al fine di suggerire contromisure per mitigare tali rischi. Si è adottato un approccio "Black Box" in quanto non si disponevano di informazioni rilevanti sulla macchina target o sulla struttura di rete. Il penetration test è stato condotto all'interno della stessa rete locale della macchina target, emulando il comportamento di un attaccante con accesso a quella rete.
—Le vulnerabilità rilevate potrebbero consentire a un utente malevolo di assumere il pieno controllo della macchina, causando danni significativi al sistema e agli utenti che utilizzano i servizi forniti da quella macchina. Ciò potrebbe compromettere la disponibilità, l'integrità e la confidenzialità del sistema. Pertanto, si può affermare che il livello di sicurezza della macchina è considerato basso, mentre il rischio di compromissione risulta essere alto. È necessario intervenire modificando il sistema ed eliminando le vulnerabilità individuate per ridurre il rischio a livelli accettabili. — Le vulnerabilità identificate, insieme alle relative contromisure, verranno elencate e descritte dettagliatamente nelle sezioni successive di questo documento.

2 Engagement Highlights

Nel contesto di questo progetto accademico, le regole di ingaggio non sono state specificate in quanto l'attività non è soggetta a accordi di non divulgazione (NDA). Non sono state imposte restrizioni riguardo agli strumenti e alle tecniche utilizzabili, a condizione che non si superasse la rete NAT creata appositamente per l'analisi della macchina target. In generale, tutto ciò che non è definito è da considerarsi non consentito, ma in questo caso non sono state imposte limitazioni. Le tecniche e gli strumenti utilizzati sono stati esplicitati nell'apposito documento.
Si è previsto che l'analisi e la redazione dei documenti relativi agli strumenti, alle metodologie utilizzate e al Penetration Testing Report richiederanno un tempo di completamento di 25 giorni lavorativi.
L'obiettivo di questa attività è limitato all'analisi della macchina target, e quindi è esplicitamente vietato ottenere informazioni tramite l'uso di metodologie di Intelligence ed è vietato coinvolgere altre persone nel processo di analisi. Durante il processo di analisi, le vulnerabilità gravi riscontrate non verranno segnalate immediatamente. Tali vulnerabilità saranno invece comunicate alla fine dell'analisi. Poiché la macchina non dispone di servizi accessibili pubblicamente, non è necessario segnalare prontamente le vulnerabilità più gravi.

3 Vulnerability Report

Secondo l'analisi effettuata, sono state individuate alcune debolezze nella macchina che la rendono suscettibile ad attacchi da parte di utenti malevoli:

- La versione del web server è affetta da molteplici vulnerabilità;
- Il web server consente l'accesso e la visualizzazione di file che non dovrebbero essere accessibili a tutti gli utenti, poiché non fanno parte dell'aspetto funzionale del sito web, ma sono spesso file di configurazione o simili che sono utili per il suo corretto funzionamento;
- Tra i file presenti sul web server, è possibile accedere all'archivio di backup, da cui è possibile risalire alle password cifrate degli utenti;
- Determinati utenti hanno accesso a file e comandi privilegiati a cui, in normali contesti, non dovrebbero poter accedere.

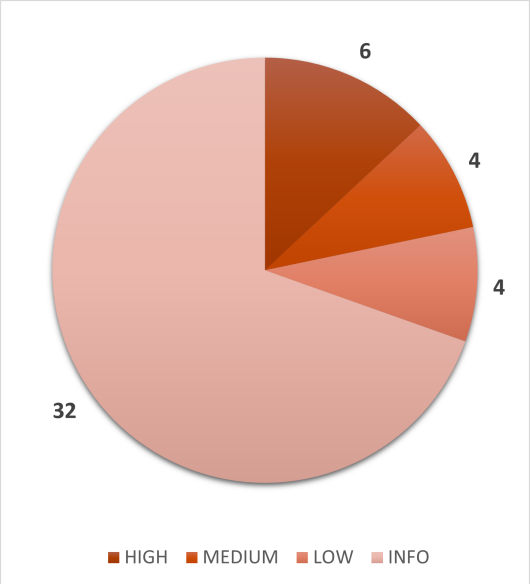
4 Remediation Report

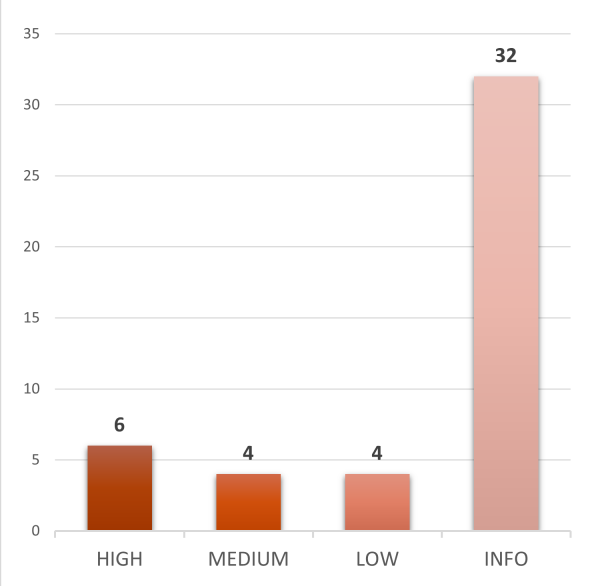
Considerando le vulnerabilità identificate durante l'attività di penetration testing, sono consigliate le seguenti strategie per migliorare la sicurezza del sistema:

- È necessario progettare e attuare un piano perfetto per la correzione delle vulnerabilità a rischio critico, alto, medio e basso. Le vulnerabilità devono essere risolte in ordine decrescente di priorità.
- Impostare corrette autorizzazioni dei file e delle directory: adottando il principio del "principio del privilegio minimo", assegnando solo i permessi necessari agli utenti e ai processi del web server.
- Mantenere l'aggiornamento e la patch del software del web server.
- Eseguire regolarmente test di sicurezza e audit.

5 Findings Summary

I seguenti grafici mostrano il numero di vulnerabilità presenti sulla macchina target sulla base della loro gravità.





6 Detailed Summary

Di seguito saranno presentate in dettaglio le vulnerabilità individuate, elencate in ordine decrescente di criticità. Inoltre, per ciascuna di esse, verranno fornite raccomandazioni specifiche per la mitigazione.

6.1 High

Information leak - CVE-2023-34981 [11]

Descrizione
Una regressione nella correzione del bug 66512 in Apache Tomcat 11.0.0-M5, 10.1.8, 9.0.74 e 8.5.88 ha causato il fatto che, se una risposta non includeva alcun header HTTP, non sarebbe stato inviato nessun messaggio AJP SEND1_HEADERS per la risposta.

Rischio
Almeno un proxy AJP (mod_proxy_ajp) utilizzerebbe le intestazioni di risposta della richiesta precedente, causando una fuga di informazioni.

Soluzione
Aggiornamento ad Apache Tomcat 9.0.75 o successivo.

Request Smuggling Vulnerability - CVE-2022-42252 [7]

Descrizione
La versione di Tomcat installata sull'host è affetta da una vulnerabilità di Request Smuggling.

Rischio
Configurando Tomcat per per ignorare gli header HTTP non validi impostando rejectIllegalHeader su false (valore non predefinito), Tomcat non respingeva una richiesta contenente un header Content-Length non valido, rendendo possibile un request smuggling attack qualora Tomcat fosse posizionato dietro a un reverse proxy che anch'esso non respingeva la richiesta con l'header non valido.

Soluzione
Aggiornamento ad Apache Tomcat 9.0.68 o successivo.

Apache Commons FileUpload - DoS - CVE-2023-24998 [9]

Descrizione
Apache Commons FileUpload prima della versione 1.5 non limita il numero di parti di richiesta da elaborare.

Rischio
Un aggressore potrebbe di innescare un DoS con un upload o una serie di upload dannosi.

Soluzione
Aggiornamento ad Apache Tomcat 9.0.71 o successivo.

Apache Tomcat EncryptInterceptorr - CVE-2022-29885 [5]

Descrizione
La documentazione di Apache Tomcat da 10.1.0-M1 a 10.1.0-M14, da 10.0.0-M1 a 10.0.20, da 9.0.13 a 9.0.62 e da 8.5.38 a 8.5.78 per EncryptInterceptor affermava erroneamente che permetteva l'esecuzione del clustering Tomcat su una rete non fidata. Questa affermazione non è corretta.

Rischio
Sebbene EncryptInterceptor fornisca una protezione della riservatezza e dell'integrità, non protegge da tutti i rischi associati all'esecuzione su una rete non attendibile, in particolare dai rischi DoS.

Soluzione
Aggiornamento ad Apache Tomcat 9.0.63 o successivo.

Denial of Service - CVE-2021-42340 [3]

Descrizione
La correzione del bug 63362 presente in Apache Tomcat da 10.1.0-M1 a 10.1.0-M5, da 10.0.0-M1 a 10.0.11, da 9.0.40 a 9.0.53 e da 8.5.60 a 8.5.71 introduce un memory leak. L'oggetto introdotto per raccogliere le metriche per le connessioni di aggiornamento HTTP non veniva rilasciato per le connessioni WebSocket una volta chiusa la connessione.

Rischio
Il memory leak poteva portare a una negazione del servizio tramite un OutOfMemoryError.

Soluzione
Aggiornamento ad Apache Tomcat 9.0.54 o successivo.

Apache Tomcat - JsonErrorReportValve injection - CVE-2022-45143 [8]

Descrizione
La JsonErrorReportValve non ha eseguito l'escape dei valori type, message o description.

Rischio
In alcune circostanze questi valori sono costruiti a partire da dati forniti dall'utente ed è quindi possibile che gli utenti forniscano valori che invalidano o manipolano l'output JSON.

Soluzione
Aggiornamento ad Apache Tomcat 9.0.69 o successivo.

6.2 Medium

Apache Tomcat - Information Disclosure - CVE-2023-28708 [10]

Descrizione
Quando si utilizza RemoteIpFilter con richieste ricevute da un reverse proxy via HTTP che includono l'intestazione XForwarded-Proto impostata su https, i cookie di sessione creati da Apache Tomcat 11.0.0-M1 a 11.0.0.-M2, da 10.1.0-M1 a 10.1.5, da 9.0.0-M1 a 9.0.71 e da 8.5.0 a 8.5.85 non includevano l'attributo secure.

Rischio
Ciò potrebbe comportare che l'agente utente trasmetta il cookie di sessione su un canale non sicuro.

Soluzione
Aggiornamento ad Apache Tomcat 9.0.72 o successivo.

Apache Tomcat - XSS in examples web application - CVE-2022-34305 [6]

Descrizione
In Apache Tomcat da 10.1.0-M1 a 10.1.0-M16, da 10.0.0-M1 a 10.0.22, da 9.0.30 a 9.0.64 e da 8.5.50 a 8.5.81 l'esempio di autenticazione Form nell'applicazione web di esempio visualizzava i dati forniti dall'utente senza filtro.

Rischio
Cross Site Scripting.

Soluzione
Aggiornamento ad Apache Tomcat 9.0.65 o successivo.

Apache Tomcat Default Files [1]

Descrizione
Il server web remoto contiene file predefiniti.

Rischio
Sul server Apache Tomcat remoto sono installati la pagina di errore predefinita, la pagina di indice predefinita, JSP di esempio e/o servlet di esempio. Questi file devono essere rimossi perché potrebbero aiutare un utente malintenzionato a scoprire informazioni sull'installazione Tomcat remota o sull'host stesso.

Soluzione
Eliminare la pagina indice predefinita e rimuovete le JSP e le servlet di esempio. Seguire le istruzioni di Tomcat o OWASP per sostituire o modificare la pagina di errore predefinita.

Manca l'intestazione anti-clickjacking [2]

Descrizione
La risposta non include né Content-Security-Policy con la direttiva "frame-ancestors" né X-Frame-Options.

Rischio
Espone l'host ad attacchi "ClickJacking".

Soluzione
I browser Web moderni supportano le intestazioni HTTP Content-Security-Policy e X-Frame-Options. Assicuratevi che una di queste sia impostata su tutte le pagine web restituite dal vostro sito/app. Se si prevede che la pagina venga inquadrata solo dalle pagine del proprio server (ad esempio, fa parte di un FRAMESET), allora si dovrà usare SAMEORIGIN, altrimenti, se non si prevede che la pagina venga inquadrata, si dovrà usare DENY. In alternativa, si può considerare l'implementazione della direttiva "frame-ancestors" di Content Security Policy.

6.3 Low

Mitigazioni Spring4Shell [4]

Descrizione
L'implementazione semplificata delle letture e delle scritture bloccanti ha messo a nudo un bug di concorrenza.

Rischio
Poteva causare la condivisione di un'istanza di Http11Processor da parte delle connessioni client, con conseguente ricezione delle risposte (o di una parte di esse), da parte del client sbagliato.

Soluzione
Aggiornamento ad Apache Tomcat 9.0.62 o successivo.

Il server web consente il completamento automatico della password

Descrizione
Il server Web remoto contiene almeno un campo modulo HTML con un input di tipo "password" in cui "completamento automatico" non è impostato su "off".

Rischio
Sebbene questo non rappresenti un rischio per il server Web in sé, significa che gli utenti che utilizzano i moduli interessati potrebbero avere le loro credenziali salvate nei loro browser, il che potrebbe a sua volta portare a una perdita di riservatezza se qualcuno di loro utilizza un host condiviso o se il loro computer viene compromesso a un certo punto.

Soluzione
Aggiungete l'attributo "autocomplete=off" a questi campi per evitare che i browser memorizzino le credenziali.

Il server web trasmette credenziali in chiaro

Descrizione
Il server Web remoto contiene diversi campi di modulo HTML contenenti un input di tipo "password" che trasmettono le loro informazioni a un server Web remoto in chiaro.

Rischio
Un aggressore che intercetta il traffico tra il browser web e il server può ottenere login e password di utenti validi.

Soluzione
Assicurarsi che ogni modulo sensibile trasmetta il contenuto tramite HTTPS.

Intestazione X-Content-Type-Options mancante [12]

Descrizione
L'intestazione Anti-MIME-Sniffing X-Content-Type-Options non è stata impostata su "nosniff".

Rischio
Ciò consente alle versioni precedenti di Internet Explorer e Chrome di eseguire il MIME-sniffing sul corpo della risposta, causando potenzialmente l'interpretazione e la visualizzazione del corpo della risposta come un tipo di contenuto diverso da quello dichiarato. Le versioni attuali (inizio 2014) e precedenti di Firefox utilizzeranno il tipo di contenuto dichiarato (se impostato), anziché eseguire il MIME-sniffing.

Soluzione
Assicurarsi che l'applicazione/server web imposti l'intestazione Content-Type in modo appropriato e che imposti l'intestazione X-Content-Type-Options su "nosniff" per tutte le pagine web.

6.4 Informative

Le vulnerabilità informative sono principalmente rilevate dagli strumenti di scansione automatica delle vulnerabilità. Tuttavia, queste vulnerabilità non vengono segnalate perché non sono considerate rilevanti per potenziali attacchi. Esse si riferiscono principalmente alla possibilità di ottenere informazioni sulle versioni dei servizi esposti, come la versione di Apache, la versione di HTTP e altri dettagli simili.

References

[1] *Apache Tomcat Default Files*. URL: https://cwiki.apache.org/confluence/display/TOMCAT/Miscellaneous#Miscellaneous-Q6.

[2] *Clickjacking Defense Cheat Sheet*. URL: https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html.

[3] *CVE-2021-42340 Denial of Service*. URL: https://lists.apache.org/thread/q33k672q3q3zf114fpf7vfoycghtsbxd.

[4] *CVE-2021-43980 Apache Tomcat - Information Disclosure*. URL: https://lists.apache.org/thread/3jjqbsp6j88b198x5.

[5] *CVE-2022-29885 Apache Tomcat EncryptInterceptor*. URL: https://lists.apache.org/thread/2b4qmhbcyqvc7dyfpjyx54c03x65vhcv.

[6] *CVE-2022-34305 Apache Tomcat - XSS in examples web application*. URL: https://lists.apache.org/thread/k04zk0nq6w57m72w5gb0r6z9ryhmvr4k.

[7] *CVE-2022-42252 Apache Tomcat - Request Smuggling*. URL: https://lists.apache.org/thread/zzcxzvqfdqn515zfs3dxb7n8gty589sq.

[8] *CVE-2022-45143 Apache Tomcat - JsonErrorReportValve injection*. URL: https://lists.apache.org/thread/yqkd183xrw3wqvnpcg3osbcryq85fkzj.

[9] *CVE-2023-24998 Apache Commons FileUpload - DoS with excessive parts*. URL: https://lists.apache.org/thread/4xl4l09mhwg4vgsk7dxqogcjrobrrdoy.

[10] *CVE-2023-28708 Apache Tomcat - Information Disclosure*. URL: https://lists.apache.org/thread/hdksc59z3s7tm39x0pp33mtwdrt8qr67.

[11] *CVE-2023-34981 Apache Tomcat - Information disclosure*. URL: https://lists.apache.org/thread/j1ksjh9m9gx1q60rtk1sbzmxhvj5h5qz.

[12] *Reducing MIME type security risks*. URL: https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)?redirectedfrom=MSDN.