



# **ARMAGEDDON**

## **Penetration Testing Report**

### **CPTS Report**

**Certified Penetration Testing Specialist (CPTS) Report**

**Gruppo:  
ARMAGEDDON**

**Umberto Favaro  
Tommaso Barbolani  
Leonardo Paglia  
Rocco Zamarco  
Marco Bagarolo  
Luca Minello  
Marco Simioni**

**Momentum**

**25 giugno 2024**

**Versione: 1.0**



## Table of Contents

1	Contatti di Incarico .....	4
2	Sintesi Esecutiva .....	5
2.1	Approccio .....	5
2.2	Ambito .....	5
2.3	Panoramica della Valutazione e Raccomandazioni .....	5
3	Sintesi della Valutazione del Penetration Test della Rete .....	7
3.1	Sintesi dei Risultati .....	7
4	Guida alla Compromissione della Rete Interna .....	9
4.1	Guida Dettagliata .....	9
5	Dettagli dei Risultati Tecnici .....	15
	Credential Leak SSH User .....	15
	Insertion of Sensitive Information Into Sent Data (javascript) .....	16
	Plaintext Storage of a Password (root) .....	18
	Missing Access Controll for Redis .....	19
	Reflected XSS .....	20
	OpenSSH Multiple Vulnerabilities .....	21
	Browsable Web Directories .....	22
	IMCP Date Disclosure .....	23
A	Appendice .....	24
A.1	Gravità dei Risultati .....	24
A.2	Host e Service Scoperti .....	25
A.3	Sottodomini Scoperti .....	26
A.4	Host Sfruttati .....	27
A.5	Utenti Compromessi .....	28
A.6	Flag Scoperti .....	29



## Dichiarazione di Riservatezza

I contenuti di questo documento sono stati sviluppati da ARMAGEDDON. ARMAGEDDON considera i contenuti di questo documento informazioni proprietarie e riservate aziendali. Queste informazioni devono essere utilizzate solo per lo scopo previsto. Questo documento non può essere rilasciato a un altro fornitore, partner commerciale o appaltatore senza il previo consenso scritto di ARMAGEDDON. Inoltre, nessuna parte di questo documento può essere comunicata, riprodotta, copiata o distribuita senza il previo consenso di ARMAGEDDON.

I contenuti di questo documento non costituiscono consulenza legale. L'offerta di servizi di ARMAGEDDON relativi a conformità, contenziosi o altri interessi legali non è intesa come consulenza legale e non deve essere interpretata come tale. La valutazione qui dettagliata riguarda un'azienda fittizia per scopi di formazione e esame, e le vulnerabilità non influenzano in alcun modo l'infrastruttura esterna o interna di ARMAGEDDON.



## 1 Contatti di Incarico

### MOMENTUM S.r.l.

**Indirizzo:**

Symbol, Via Cefalonia, 55, 25124 Brescia BS

**Telefono:**

030 238 8551

**Email:**

info@momentum.com

**Web:**

momentum.com

Contatti Momentum		
Contatti	Ruolo	Email
Marco Negro	CEO	marco.negro@momentum.com
Jacopo Talamini	CTO	jacopo.talamini@momentum.com

Contatti ARMAGEDDON		
Contatti	Ruolo	Email
Umberto Favaro	Cyber Security Specialist	umberto.favaro@armageddon.pt
Tommaso Barbolani	Cyber Security Specialist	tommaso.barbolani@armageddon.pt
Leonardo Paglia	Cyber Security Specialist	leonardo.paglia@armageddon.pt
Rocco Zamarco	Cyber Security Specialist	rocco.zamarco@armageddon.pt
Marco Bagarolo	Cyber Security Specialist	marco.bagarolo@armageddon.pt
Luca Minello	Cyber Security Specialist	luca.minello@armageddon.pt
Marco Simioni	Cyber Security Specialist	marco.simioni@armageddon.pt



## 2 Sintesi Esecutiva

Momentum ("Momentum" nel seguito) ha incaricato ARMAGEDDON di eseguire un Penetration Test della rete interna di Momentum per identificare le vulnerabilità di sicurezza, determinare l'impatto su Momentum, documentare tutti i risultati in modo chiaro e ripetibile, e fornire raccomandazioni per la rimedio.

### 2.1 Approccio

ARMAGEDDON ha eseguito i test il 25 giugno 2024 in modalità Black Box, ossia senza credenziali o alcuna conoscenza preliminare dell'ambiente esterno di Momentum con l'obiettivo di identificare vulnerabilità sconosciute. I test sono stati eseguiti da un punto di vista non invasivo con l'obiettivo di scoprire il maggior numero possibile di configurazioni errate e vulnerabilità. I test sono stati eseguiti da remoto dai laboratori di valutazione di ARMAGEDDON. Ogni vulnerabilità identificata è stata documentata e indagata manualmente per determinare le possibilità di sfruttamento e il potenziale di escalation. ARMAGEDDON ha cercato di dimostrare il pieno impatto di ogni vulnerabilità. Se ARMAGEDDON fosse riuscito a ottenere un punto d'appoggio nella rete interna, Momentum a seguito del test della rete esterna, Momentum ha consentito ulteriori test inclusi movimenti laterali e escalation di privilegi orizzontale/verticale per dimostrare l'impatto di un compromesso della rete interna.

### 2.2 Ambito

L'ambito di questa valutazione includeva un indirizzo IP interno, un range di ip della rete interna, e qualsiasi altro servizio o posseduto da Momentum scoperto in caso di accesso alla rete interna.

### In Scope Assets

Host/URL/IP Address	Description
192.168.56.105	Webapp pubblica(Momentum)

### 2.3 Panoramica della Valutazione e Raccomandazioni

Durante il penetration test contro Momentum, ARMAGEDDON ha identificato 8 vulnerabilità che minacciano la riservatezza, l'integrità e la disponibilità dei sistemi informativi di Momentum. Le vulnerabilità sono state categorizzate per livello di gravità, con 1 delle vulnerabilità assegnate a un livello di rischio critico, ad alto rischio, 2 a medio rischio e 1 a basso rischio. C'erano anche 0 vulnerabilità informative relative al miglioramento delle capacità di monitoraggio della sicurezza all'interno della rete interna.

Nel complesso l'azienda WeakCorp ha bisogno di mettere in campo misure correttive della propria postura di cybersecurity.

Momentum dovrebbe creare un piano di rimedio basato sulla sezione Riepilogo delle azioni correttive di questo rapporto, affrontando tutte le vulnerabilità ad alto rischio il prima possibile secondo le



# ARMAGEDDON

---

esigenze dell'azienda. Momentum dovrebbe anche considerare di eseguire valutazioni periodiche delle vulnerabilità se non vengono già eseguite.



## 3 Sintesi della Valutazione del Penetration Test della Rete

### 3.1 Sintesi dei Risultati

Durante il corso del test, ARMAGEDDON ha scoperto un totale di 8 vulnerabilità che rappresentano un rischio significativo per i sistemi informativi di Momentum. ARMAGEDDON ha anche identificato 0 vulnerabilità informative che, se affrontate, potrebbero rafforzare ulteriormente la postura complessiva di sicurezza di Momentum. Le vulnerabilità informative sono osservazioni per aree di miglioramento dell'organizzazione e non rappresentano di per sé vulnerabilità di sicurezza. Il grafico sottostante fornisce un riepilogo delle vulnerabilità per livello di gravità.

Nel corso di questo Penetration Test **1 Critico**, **4 High**, **2 Medio** and **1 Basso** sono state identificate vulnerabilità:

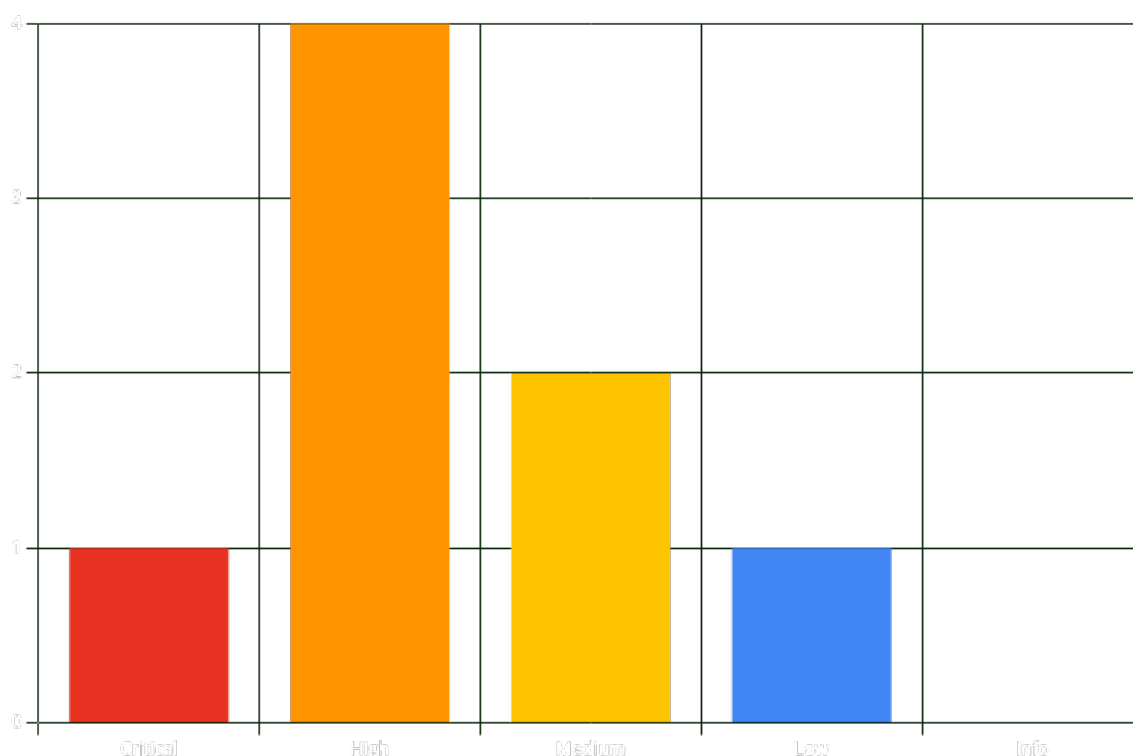


Figure 1 - Distribuzione delle vulnerabilità identificate

Di seguito è riportata una panoramica ad alto livello di ciascun risultato identificato durante i test. Questi risultati sono trattati in dettaglio nel Dettaglio dei Risultati Tecnici sezione di questo report.

#	Livello di Gravità	Nome del Risultato	Pagina
1	10.0 (Critical)	Credential Leak SSH User	15
2	8.6 (High)	Insertion of Sensitive Information Into Sent Data (javascript)	16
3	8.4 (High)	Plaintext Storage of a Password (root)	18



# ARMAGEDDON

#	Livello di Gravità	Nome del Risultato	Pagina
4	8.3 (High)	Missing Access Controll for Redis	19
5	7.5 (High)	Reflected XSS	20
6	6.4 (Medium)	OpenSSH Multiple Vulnerabilities	21
7	4.3 (Medium)	Browsable Web Directories	22
8	3.7 (Low)	IMCP Date Disclosure	23





## 4 Guida alla Compromissione della Rete Interna

### 4.1 Guida Dettagliata

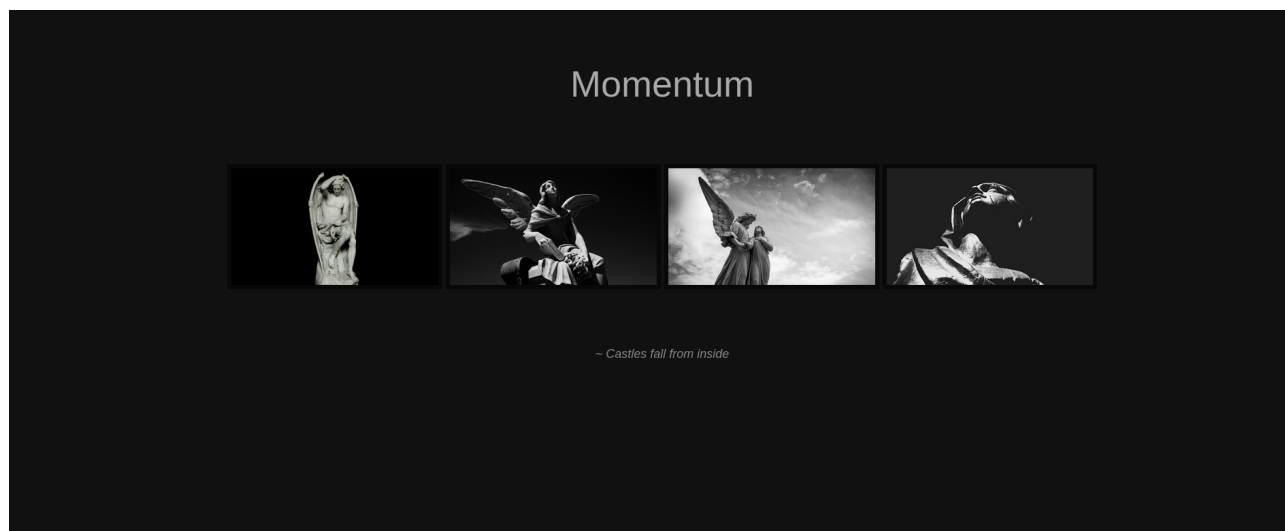
Per iniziare ci avvaliamo di nmap per individuare che le porte 22 e 80 sono esposte.

```
nmap -p- 192.168.56.105
```

```
Nmap scan report for 192.168.56.105
Host is up (0.00091s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 08:00:27:1D:D7:D5 (Oracle VirtualBox virtual NIC)
```

Arrivati a questo punto, data la presenza della porta 80(HTTP) aperta, ci siamo collegati da browser allo stesso indirizzo.

Da qui veniamo a conoscenza di una pagina una pagina statica con delle foto di varie statue



Adesso procediamo a scansionare con dirb eventuali cartelle e/o file nascosti.

Tra i vari percorsi trovati notiamo una sub-directory in particolare, denominata "js", la quale contiene a sua volta il file "main.js".

Al suo interno possiamo vedere il seguente codice:



```
function viewDetails(str) {  
    window.location.href = "opus-details.php?id="+str;  
}  
  
/*  
var CryptoJS = require("crypto-js");  
var decrypted = CryptoJS.AES.decrypt(encrypted, "SecretPassphraseMomentum");  
console.log(decrypted.toString(CryptoJS.enc.Utf8));  
*/
```

Da quanto mostrato, si nota la presenza del file opus-details.php. Questo mostra un'output di testo o pagine diverse in base all' ID variabile inserito nel link dopo l'estensione "?ID=...". Subito sotto è presente una parte in cui viene mostrato il processo di decriptazione, tramite la funzione cryptojs, la quale utilizza la stringa "SecretPassphraseMomentum".

In seguito, abbiamo analizzato la risposta della pagina web, è stato rilevato che il sito rilascia un cookie al client senza apparente motivo.




Browser tabs: Momentum | Index, Momentum | Details, Momentum | Details, Module Index - Ap

Address bar: 192.168.56.106/opus-details.php?id=angel

Browser bookmarks: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec

**Momentum**



*id : angel*

*Name : Santa María Magdalena de Pazzi*

Inspector, Console, Debugger, Network, Style Editor, Performance, Memory, Storage

Filter Items	Name	Value	Domain	Path	Expires / M
cookie	U2FsdGVkX193...	192.168.56.1...	/opus-d...	Session	

Filter values

▼ Data

▼ cookie: "U2FsdGVkX193yTOKO...qGuQ6Mx28N1VbBSZt"

Created: "Tue, 25 Jun 2024 08:34:23 GMT"

Domain: "192.168.56.106"

Expires / Max-Age: "Session"

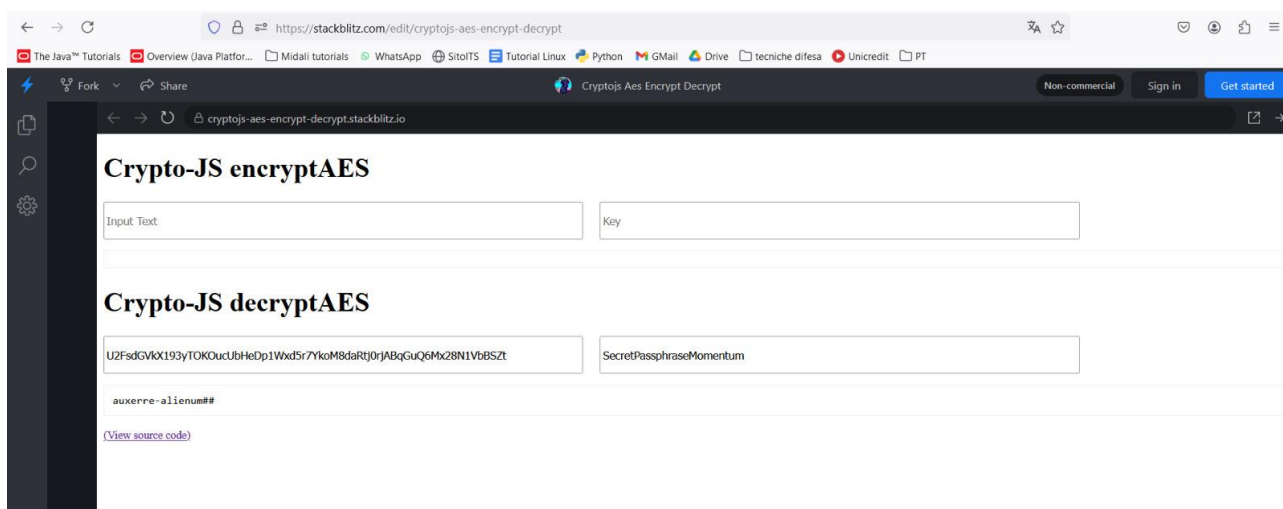
HostOnly: true

HttpOnly: false

Last Accessed: "Tue, 25 Jun 2024 09:11:45 GMT"

Path: "/opus-details.php"

Unendo le due informazioni arriviamo alla conclusione che è possibile decriptare il cookie sfruttando l'algoritmo AES con la chiave "SecretPassphraseMomentum". Per svolgere questa attività abbiamo utilizzato un sito per la decriptazione AES.



Il risultato è una stringa, che dopo una serie di tentativi, abbiamo scoperto essere la combinazione di username e password da utilizzare per connetterci in SSH. Il nome utente è "auxerre" e la password è la stringa completa, ossia "auxerre-alienum##".

Una volta che ci siamo connessi con successo alla porta 22, è stato immediato cercare la flag sulla home dell'utente con un semplice "ls". Dentro il file "user.txt" si presenta così:

```
auxerre@Momentum:~$ cat user.txt
[ Momentum - User Owned ]

flag : 84157165c30ad34d18945b647ec7f647

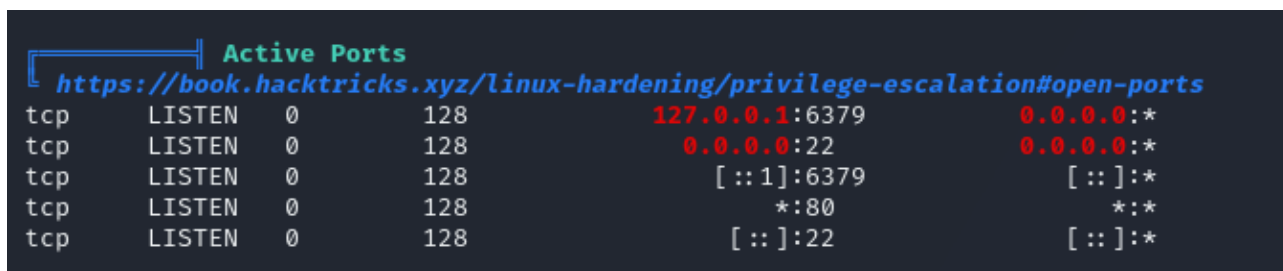
auxerre@Momentum:~$
```

La flag quindi è 84157165c30ad34d18945b647ec7f647.

Da questo punto proseguiamo con l'installazione dello strumento linpeas con lo scopo di trovare una via per ottenere l'accesso da amministratore. Per farlo abbiamo copiato dal sito linpeas.sh il codice del tool, per poi incollarlo in un file creato sulla macchina target.

Dopo aver dato i permessi di esecuzione al file con il comando `chmod +x linpeas.sh`, abbiamo eseguito lo strumento.

Questo ci ha permesso di trovare una falla di sicurezza: il servizio "Redis" sulla porta interna 6379 è accessibile e senza password.





```
Analyzing Redis Files (limit 70)
Redis server v=5.0.3 sha=00000000:0 malloc=jemalloc-5.1.0 bits=64 build=94145a25ce04923
Redis isn't password protected
-rw-r----- 1 redis redis 62226 Feb 25 2021 /etc/redis/redis.conf
```

Prima di proseguire ci informiamo su Redis e le sue vulnerabilità.

Redis è un database NoSQL di tipo "key/value storage". Esso si basa infatti su una struttura a dizionario: ogni valore immagazzinato è abbinato ad una chiave univoca che ne permette il recupero.

Proseguiamo quindi a collegarci al servizio con il comando "redis-cli" stabilendo una connessione al database Redis locale.

Successivamente, il comando INFO keypace ha rivelato la presenza di una chiave nel database. Abbiamo quindi eseguito il comando KEYS \*, che ha elencato tutte le chiavi presenti, tra cui la chiave "rootpass".

Infine, abbiamo utilizzato il comando GET rootpass per recuperare il valore associato a questa chiave, che si è rivelato essere la password di root in chiaro: "**m0mentum-allenum##**".

```
(kali㉿kali)-[~]
$ ssh auxerre@172.31.80.38
auxerre@172.31.80.38's password:
Linux Momentum 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jun 25 06:37:33 2024 from 172.31.80.28
auxerre@Momentum:~$ redis-cli
127.0.0.1:6379> INFO keypace
# Keyspace
db0:keys=1,expires=0,avg_ttl=0
127.0.0.1:6379> SELECT 0
OK
127.0.0.1:6379> KEYS *
1) "rootpass"
127.0.0.1:6379> Get rootpass
"m0mentum-allenum##"
127.0.0.1:6379> █
```

Successivamente, avendo ottenuto le credenziali di root, abbiamo effettuato l'accesso al sistema eseguendo il comando "su" nel terminale e inserendo la password appena scoperta.

Navigando tra le cartelle abbiamo poi ottenuto la flag aprendo il file root.txt.



# ARMAGEDDON

```
auxerre@Momentum:/$ su root
Password:
root@Momentum:/# ls
bin  dev  home  initrd.img.old  lib32  libx32  media  opt  root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lib  lib64  lost+found  mnt  proc  run  srv  tmp  var  vmlinuz.old
root@Momentum:/# cd root
root@Momentum:~# ls
root.txt
root@Momentum:~# cat root.txt
[ Momentum - Rooted ]
_____
Flag : 658ff660fdac0b079ea78238e5996e40
_____
by alienum with <3
```

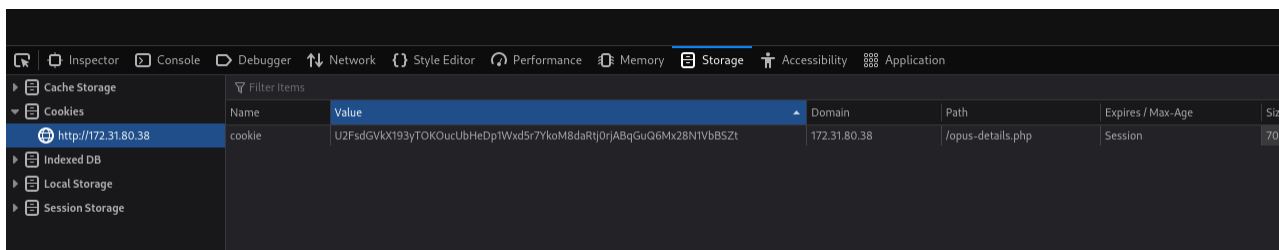
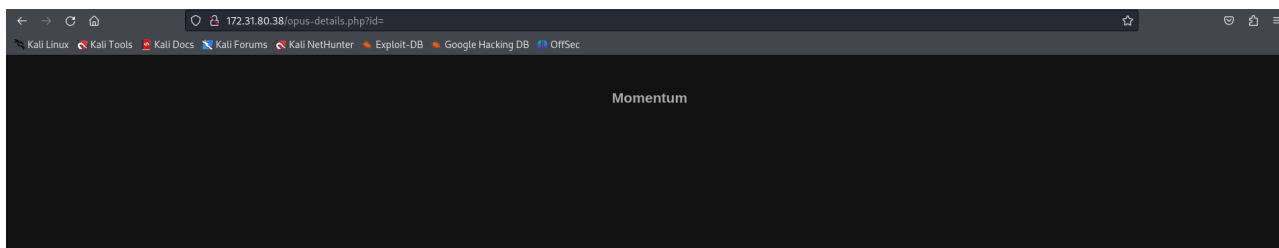


## 5 Dettagli dei Risultati Tecnici

### 1. Credential Leak SSH User - Critical

CWE	CWE-200
CVSS 3.1	10.0 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L
Causa Principale	Navigando alla pagina /opus-details.php viene aggiunto allo user un cookie contenente come valore la password ssh dell'account auxerre, anche se criptata
Impatto	Impatto Critico, anche se criptata è sempre una password importante della macchina che viene consegnata solamente navigando per il sito web
Componente Interessato	User Account
Rimedi	Eliminare l'assegnazione del cookie con urgenza
Riferimenti	-

### Evidenze Trovate





## 2. Insertion of Sensitive Information Into Sent Data (javascript) - High

CWE	CWE 201
CVSS 3.1	8.6 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
Causa Principale	All'interno del file /js/main.js sono contenute informazioni critiche che permettono a un utente malintenzionato di rompere la crittografia dei dati del sito  /* var CryptoJS = require("crypto-js"); var decrypted = CryptoJS.AES.decrypt(encrypted, "SecretPassphraseMomentum"); console.log(decrypted.toString(CryptoJS.enc.Utf8)); */ la chiave privata "SecretPassphraseMomentum" dell'algoritmo di crittazione aes
Impatto	Impatto Alto all'interno di quel file può facilmente decriptare dati del sito riuscendo a ottenere a informazioni protette.
Componente Interessato	Cypher mechanism
Rimedi	Togliere i commenti contenenti informazioni sensibili.
Riferimenti	-

## Evidenze Trovate

The screenshot displays the Burp Suite interface. The top pane shows a list of sites, with 'http://192.168.56.107' selected. The middle pane shows the 'Request' tab for a GET request to '/js/main.js'. The response body contains JavaScript code that decrypts a sensitive string using CryptoJS. The bottom pane shows a list of requests, with 'GET: http://192.168.56.107/js/main.js' selected. The right pane shows a security alert titled 'Server Leaks Version Information via "Server" HTTP Response Header Field', indicating a low risk of information disclosure.

File Edit View Analyse Report Tools Import Export Online Help

Standard Mode

Sites +

Quick Start Request Response Requester +

Header: Text Body: Text

HTTP/1.1 200 OK  
Date: Tue, 25 Jun 2024 07:54:27 GMT  
Server: Apache/2.4.38 (Debian)  
Last-Modified: Thu, 22 Apr 2021 04:59:54 GMT  
ETag: "10b-5c0888cc680"  
Accept-Ranges: bytes

```
function viewDetails(str) {  
    window.location.href = "opus-details.php?id="+str;  
}  
  
/*  
var CryptoJS = require("crypto-js");  
var decrypted = CryptoJS.AES.decrypt(encrypted, "SecretPassphraseMomentum");  
console.log(decrypted.toString(CryptoJS.enc.Utf8));  
*/
```

History Search Alerts Output Spider Active Scan +

GET: http://192.168.56.107/robots.txt  
GET: http://192.168.56.107/js/main.js

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

URL: http://192.168.56.107/js/main.js  
Risk: Low  
Confidence: High  
Parameter:  
Attack:  
Evidence: Apache/2.4.38 (Debian)  
CWE ID: 200  
WASC ID: 13  
Source: Passive (10036 - HTTP Server Response Header)





# ARMAGEDDON

```
function viewDetails(str) {  
    window.location.href = "opus-details.php?id="+str;  
}  
  
/*  
var CryptoJS = require("crypto-js");  
var decrypted = CryptoJS.AES.decrypt(encrypted, "SecretPassphraseMomentum");  
console.log(decrypted.toString(CryptoJS.enc.Utf8));  
*/
```

## Crypto-JS decryptAES

[\(View source code\)](#)



## 3. Plaintext Storage of a Password (root) - High

CWE	CWE-256
CVSS 3.1	8.4 / CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:H/RL:O/RC:C/CR:H/IR:H/AR:L/MAV:L/MAC:L/MPR:L/MUI:N/MS:C/MC:H/MI:H/MA:H
Causa Principale	All'interno di un database di Redis c'è una chiave (record) che contiene la password dell'utente root in chiaro.
Impatto	Impatto Alto un utente malintenzionato che ottiene accesso al database otterrà immediatamente accesso alla password di root.
Componente Interessato	<ul style="list-style-type: none"><li>• Redis Database</li><li>• Credenziali utente root</li></ul>
Rimedi	Implementare un password manager per salvare le password mai salvarle in chiaro.
Riferimenti	-

### Evidenze Trovate

```
INFO keyspace
SELECT 0
KEYS *
Get rootpass
```

```
127.0.0.1:6379> INFO keyspace
# Keyspace
db0:keys=1,expires=0,avg_ttl=0
127.0.0.1:6379> SELECT 0
OK
127.0.0.1:6379> █
```

```
127.0.0.1:6379> KEYS *
1) "rootpass"
127.0.0.1:6379> █
```



## 4. Missing Access Control for Redis - High

CWE	CWE 306
CVSS 3.1	8.3 / CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L
Causa Principale	La macchina ha il servizio Redis attivo nella porta 6379 e qualunque connessione che passa attraverso localhost (127.0.0.1) può collegarsi in modo anonimo senza credenziali o autenticazione.
Impatto	Impatto Medio-Alto accedendo a questo servizio un malintenzionato ha accesso a l'intero contenuto del database di Redis e potrebbe essere ulteriormente utilizzato per eseguire comandi o caricare una webshell con privilegi elevati.
Componente Interessato	<ul style="list-style-type: none"><li>• Servizio Redis</li><li>• Database Redis</li></ul>
Rimedi	Implementare un meccanismo di controllo degli accessi anche semplicemente username e password.
Riferimenti	-

### Evidenze Trovate

```
redis-cli
```

```
auxerre@Momentum:~$ chmod +x pspy64.py
auxerre@Momentum:~$ redis-cli
127.0.0.1:6379>
```

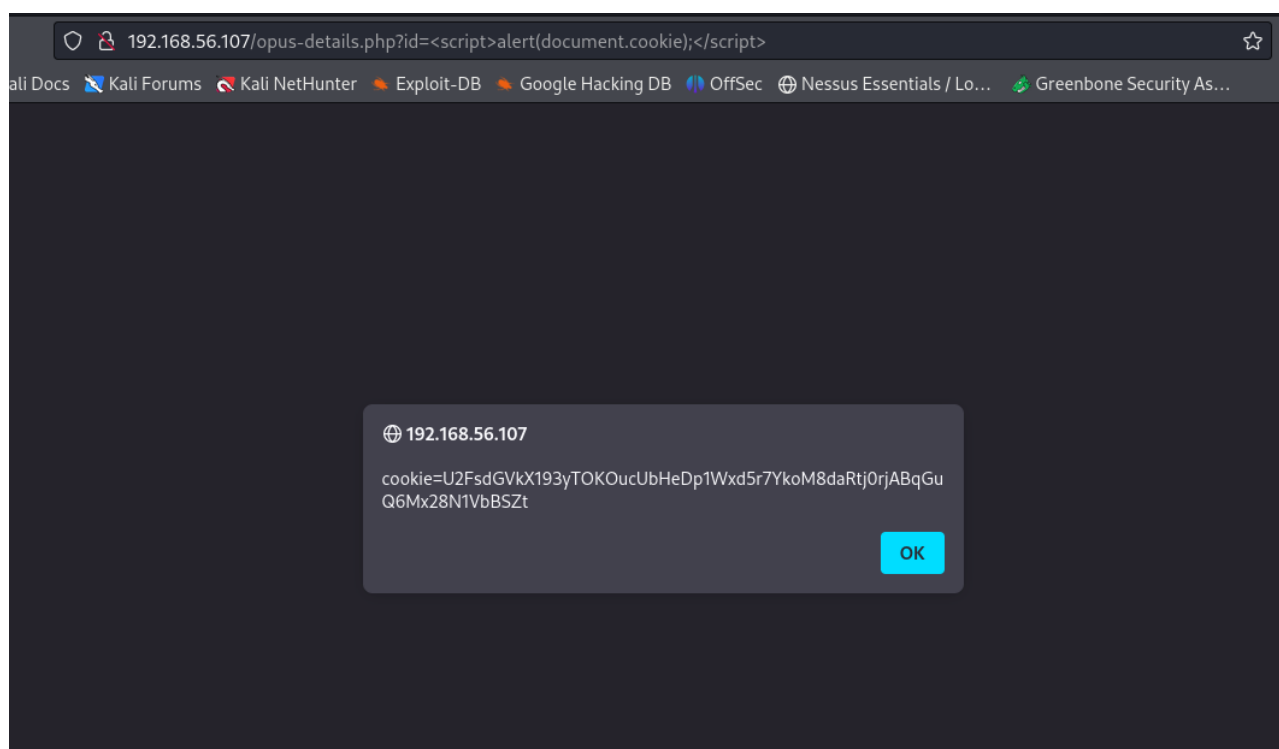


## 5. Reflected XSS - High

CWE	CWE 79
CVSS 3.1	7.5 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
Causa Principale	Non è presente nessun tipo di sanitazione degli input, header di sicurezza, Content security policy o altri metodi per bloccare cross site script è perciò sufficiente inserire il payload <code>&lt;[script]&gt;alert(document.cookie);&lt;/[script]&gt;</code> nell'endpoint <code>/opus-details.php?id=</code>
Impatto	Impatto medio un malintenzionato può creare un link malevolo che se passato a un utente esegue codice arbitrario nella sua macchina.
Componente Interessato	<ul style="list-style-type: none"><li>• Users machine</li><li>• Website</li></ul>
Rimedi	Applicare CSP e header di sicurezza per mitigare cross site scripting
Riferimenti	-

### Evidenze Trovate

`http://192.168.56.107/opus-details.php?id=%3Cscript%3Ealert(document.cookie);%3C/script%3E`





## 6. OpenSSH Multiple Vulnerabilities - Medium

CWE	CWE 1329
CVSS 3.1	6.4 / CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:L
Causa Principale	La versione in uso di OpenSSH è 7.9p1 è obsoleto e vulnerabile alle seguenti: SSH Terrapin Prefix Truncation Weakness CVE-2023-48795 OS Command Injection CVE-2023-6004 OS Command Injection Git repo CVE-2023-51385 No sanitization Inadequate encryption strength CVE-2023-51384
Impatto	Impatto medio alto le vulnerabilità presenti possono consentire di ottenere informazioni non
Componente Interessato	<ul style="list-style-type: none"><li>• OS</li><li>• OpenSSH</li></ul>
Rimedi	Aggiorna OpenSSH a l'ultima versione sicura.
Riferimenti	-








## 7. Browseable Web Directories - Medium

CWE	CWE 200
CVSS 3.1	4.3 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O/RC:U
Causa Principale	Le cartelle /js/, /img/, /css/ e /manual/ della webapp sono navigabili.
Impatto	Impatto Medio informazioni sul funzionamento del sito vengono rilasciate
Componente Interessato	Webapp
Rimedi	Impostare restrizioni dell'accesso o impedire che le cartelle mostrino dati sensibili.
Riferimenti	-

### Evidenze Trovate

## Index of /img

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">a.jpg</a>	2021-04-19 19:59	489K	
 <a href="#">b.jpg</a>	2021-04-19 19:59	313K	
 <a href="#">c.jpg</a>	2021-04-19 19:55	217K	
 <a href="#">d.jpg</a>	2021-04-20 03:01	22K	

*Apache/2.4.38 (Debian) Server at 192.168.56.107 Port 80*



## 8. ICMP Date Disclosure - Low

CWE	CWE 2000
CVSS 3.1	3.7 / CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:U/RL:O/RC:U/CR:L/IR:L/AR:L/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:L/MI:N/MA:N
Causa Principale	L'host remoto risponde a una richiesta di timestamp ICMP. Questo permette a un attaccante di conoscere la data impostata sulla macchina bersaglio
Impatto	Impatto basso informazioni di sistema come l'ora della macchina possono essere utili a tentare di forzare la crittazione.
Componente Interessato	<ul style="list-style-type: none"><li>• Protocollo ICMP</li><li>• Network</li></ul>
Rimedi	Filtrare le richieste ICMP timestamp e le risposte ICMP timestamp in uscita.
Riferimenti	-



## A Appendice

### A.1 Gravità dei Risultati

Ad ogni risultato è stata assegnata una gravità critica, alta, media, bassa o informativa. La valutazione si basa sulla priorità con cui ogni risultato dovrebbe essere considerato e sul potenziale impatto che ciascuno ha sulla riservatezza, integrità e disponibilità dei dati di Momentum.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0





## A.2 Host e Service Scoperti

IP Address	Port	Service	Notes
192.168.56.105	80	Apache httpd 2.4.38((Debian))	
192.168.56.105	22	OpenSSH 7.9p1	



## A.3 Sottodomini Scoperti

URL	Description	Discovery Method
192.168.56.105/js/main.js	CryptoJS script	HTML code inspection



## A.4 Host Sfruttati

Host	Scope	Method	Notes
192.168.56.105:80	Momentum	Web	Null



## A.5 Utenti Compromessi

Username	Type	Method	Notes
auxerre	SSH	Password discovery	2nd vulnerability
root	SSH	Password discovery	4th vulnerability



## A.6 Flag Scoperti

User	Flag
user.txt	84157165c30ad34d18945b647ec7f647
root.txt	658ff660fdac0b079ea78238e5996e40



*Fine Documentazione*

*Questo report è stato redatto  
da ARMAGEDDON con*



*Umberto Favaro  
Tommaso Barbolani  
Leonardo Paglia  
Rocco Zamarco  
Marco Bagarolo  
Luca Minello  
Marco Simioni*