



# MOMENTUM CTF by ARMAGEDDON

Bagarolo Marco, Barbolani di Montauto Tommaso, Favaro Umberto  
Minello Luca, Paglia Leonardo, Simioni Marco, Zamarco Rocco Orso Maria



# SOMMARIO DEL TARGET

## 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)

# LE VULNERABILITA'

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

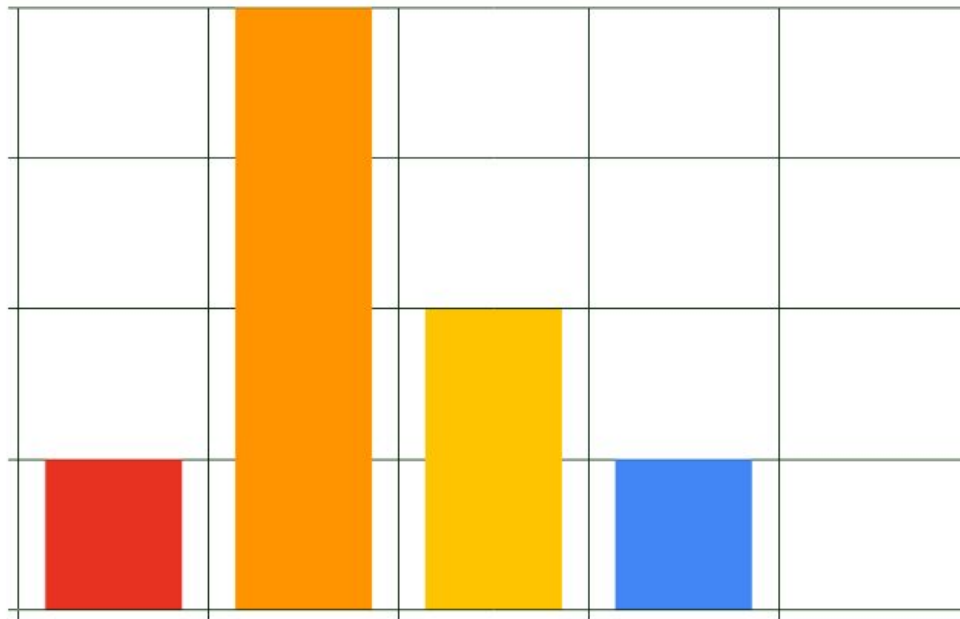



Figure 1 - Distribuzione delle vulnerabilità identificate



#	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

#	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 Vulnerability	21
7	4.3 (Medium)	Browsable Web Directories	22
8	3.7 (Low)	IMCP Date Disclosure	23