





22 · 08

2021

JamalSec srl

WEB APPLICATION ASSESSMENT

Indice

1	Patto di Riservatezza	3
1.1	Bilateralità	3
1.2	Scopo	3
1.3	Durata	3
1.4	Condivisione con terze parti	3
2	Esclusione delle Responsabilità	3
3	Contatti 	4
3.1	JamalSec srl	4
3.2	Cliente	4
4	RISULTATI 	5
4.1	Legenda	5
5	Sintesi (EXECUTIVE SUMMARY)	5
5.1	Riepilogo attacco	5
5.2	Altri dettagli	5
6	VAPT: DETTAGLI TECNICI 	6
6.1	Ricognizione	6
6.2	Shell www-data	6
6.3	Privilege Escalation	6
6.4	SISTEMA LINUX (IP: 192.168.0.0)	7
6.4.1	Enumerazione Servizi	7
6.4.2	Vulnerability Explanation	7
6.4.3	Fix Vulnerabilita	7
6.4.4	Proof of Concept Code	7
6.4.5	Shell Screenshot	7
6.4.6	Elevazione Privilegi	7
6.4.7	Descrizione Vulnerabilita'	7
6.5	PASSWORD DATA BREACH	8
6.5.1	PROOF OF CONCEPT	8
6.5.2	MITIGAZIONE 	8

1 Patto di Riservatezza

Il presente documento è di proprietà esclusiva di JamalSec srl e Gioielleria Vairo di Pasquale.
Le informazioni contenute in questo documento sono di natura esclusiva e riservata.

1.1 Bilateralità

Entrambe le parti sono vincolate al rispetto del patto di riservatezza.

1.2 Scopo

L'uso delle informazioni contenute nel documento è limitato alla valutazione dei sistemi informatici di Gioielleria Vairo di Paquale.

1.3 Durata

Il patto di riservatezza ha una durata limitata nel tempo, la validità del patto termina il 31 dicembre 2020 alle ore 23 e 59 minuti.

1.4 Condivisione con terze parti

Gioielleria Vairo di Pasquale può condividere le informazioni con i propri dipendenti e consulenti, previa autorizzazione esplicita di JamalSec srl.

La copiatura, divulgazione o uso, per intero o in parte, richiede un consenso esplicito da parte di JamalSec e Gioielleria Vairo di Pasquale.

2 Esclusione delle Responsabilità

Un VAPT (Vulnerability Assestment, Penetration Test) è da considerarsi come **un'istantanea nel tempo** dell'oggetto target.
I risultati dei test e le raccomandazioni proposte, riflettono le informazioni raccolte durante la valutazione e non eventuali cambiamenti o modifiche apportate al di fuori di tale periodo.

Gli impegni a tempo limitato non consentono una valutazione completa di tutti i controlli di sicurezza.







JamalSec srl ha dato la priorità allo svolgimento di controlli di sicurezza per indentificare i punti più deboli che un utente malintenzionato avrebbe sfruttato.

JamalSec srl raccomanda di condurre valutazioni simili su base annuale da tester interni o di terze parti per garantire continuità ed efficacia dei controlli.

3 Contatti

3.1 JamalSec srl

 VIA LEMANI DARCULO 4, PESARO

Daniele Ravaglia	CEO	 +39 051 12345  driver@clock.it
Michele di Stefano	Senior Pentester	 +39 051 12345  theBoss@pwc.it
Diego de Angelis	Stagista schiavo	 +39 051 12345  ravaglia8me@pwc.it

3.2 Cliente

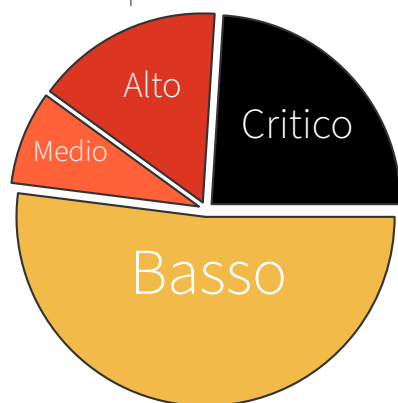
 VIA NARA STABBOCCHI 69, CODROIPO

Vairo di Pasquale	CEO	 +39 051 12345  theBoss@pwc.it
-------------------	-----	---

4 RISULTATI

Le vulnerabilità emerse dall'analisi sono classificate con lo standard CVSS v3.1:

N°	SEVERITÀ (CVSS)
6	CRITICO 9.0–10.0
4	ALTO 7.0–8.9
2	MEDIO 4.0–6.9
13	BASSO 0.1–3.9
123	INFO 0.0



4.1 Legenda

CRITICO: Vulnerabilità facilmente sfruttabili che permettono di ottenere accesso completo ai sistemi. Si consiglia di prendere provvedimenti immediati.

ALTO: Vulnerabilità il cui sfruttamento è più difficile ma causano perdita di dati o elevazione di privilegi dell'attaccante. Si consiglia di prendere provvedimenti il prima possibile.

MEDIO: Vulnerabilità che vengono rilevate ma il cui sfruttamento richiede particolari condizioni (come social engineering). Tali problemi vanno risolti dopo le categorie di maggior rischio.

BASSO: Vulnerabilità poco dannose, tuttavia la loro risoluzione riduce la superficie d'attacco. Prendere provvedimenti nel prossimo ciclo di sviluppo.

INFO: Categoria che racchiude informazioni aggiuntive raccolte durante i test o documentazione.

5 Sintesi (EXECUTIVE SUMMARY)

JamalSec ha eseguito test per la **valutazione della sicurezza del sito web della Gioielleria Vairo di Pasquale** a partire dalla data 1 Dic. 2020 fino al 31 Dic. 2020.

Tramite una serie di attacchi **sono state trovate molte vulnerabilità critiche** che hanno permesso **l'accesso completo al server remoto con conseguente furto di dati e possibili danni economici**.

Si consiglia di risolvere al più presto tali vulnerabilità in quanto facilmente individuabili da potenziali malintenzionati.

5.1 Riepilogo attacco

1. E' stata acquisita la password del pannello di amministrazione del webserver tramite ricerca della mail nei data breach pubblici.
❗ Si raccomanda di non usare la mail e username di lavoro per registrarsi in servizi terzi.
2. Dal pannello di amministrazione e' stato possibile **acquisire le password degli utenti** salvate nel database. Tali password erano **direttamente leggibili** senza bisogno di effettuare cracking.
❗ Si raccomanda di non salvare in chiaro le credenziali nei database ma usare tecniche di hashing.
3. Sfruttando un upload di file non propriamente ristretto all'interno del pannello di amministrazione, e' stato possibile caricare un file nel server che ha permesso un **accesso con privilegi limitati nel server**.
❗ Si raccomanda di applicare le restrizioni per l'upload di file indicate dalla fondazione owasp.
4. **Una versione datata del sistema operativo** installato nel server (Linux 3.4.5) ha reso possibile la elevazione dei privilegi sfruttando una vulnerabilità nota (CVE-2013-4345) e quindi e' stato ottenuto il controllo completo del server.
❗ Si raccomanda di eseguire periodici aggiornamenti di versione del sistema in uso.

5.2 Altri dettagli

Misure sicurezza trovate, da rinforzare...

6 **VAPT: DETTAGLI TECNICI**

Narrativa attacco svolto

6.1 Ricognizione

6.2 Shell www-data

6.3 Privilege Escalation

6.4 SISTEMA LINUX (IP: 192.168.0.0)

6.4.1 Enumerazione Servizi

Nmap Scan Results

```
nmap -sV -sC 10.10.10.10
```

open TCP ports	open UDP Ports
21,22,23	100,101

Come mostrato dall'immagine sopra, il sistema target ha un webserver sulla porta 80 che...

6.4.2 Vulnerability Explanation

Ability Server 2.34 e' vulnerabile ad un buffer overflow che causa esecuzione arbitraria di codice...

Severita': Critica

6.4.3 Fix Vulnerabilita

E' possibile installare una patch per questa vulnerabilita' al seguente [Link](#)

6.4.4 Proof of Concept Code

Il sorgente dell'exploit e' reperibile con `searchsploit -m 10204.py`. Ogni modifica al codice viene evidenziata in rosso. Si ricorda di cambiare opportunamente, dove necessario, gli indirizzi ip e porta rispetto a quelli della propria macchina locale in uso. Preparare, se necessario, un listener netcat con: `nc -lnvp <PORT>`.

```
1  from os import dunno
2  this.foo("fighters")
3
4  while a < 99:
5      a += 20
6
7  with open("file.txt") as f:
8      readline(f)
9      echo 'something'
10
```

Dopo aver eseguito l'exploit si dovrebbe ricevere una reverse shell come utente www-data

6.4.5 Shell Screenshot

6.4.6 Elevazione Privilegi

C'e' un cronjob lanciato come root...

6.4.7 Descrizione Vulnerabilita'

Severita': Critica

6.5 **PASSWORD DATA BREACH**

SEVERITÀ	Critico
DESCRIZIONE	È stata trovata una password associata alla email colloquio@among.us in databreach pubblici. La stessa password è stata riutilizzata per il pannello di login di amministrazione.
DOVE	http://gioielleriaProteins.com/admin-login.php
RIFERIMENTI	dehashed.com

6.5.1 **PROOF OF CONCEPT**

ACQUISIZIONE PASSWORD DAI BREACH

DIMOSTRAZIONE VALIDITÀ CREDENZIALI

6.5.2 **MITIGAZIONE** 🔧

Si consiglia di cambiare la password utilizzata per l'accesso al pannello, con una sicura (più di 14 caratteri casuali fra a-Z 0-9 e caratteri speciali). Non utilizzare la nuova password altrove.

Inoltre JamalSec raccomanda Gioielleria Vairo di Pasquale di:

- Sensibilizzare i dipendenti sull'uso sicuro di password.
- Controllare le email/password dei dipendenti in databreach pubblici.
- Disincentivare i dipendenti ad iscriversi in servizi web con la mail aziendale a meno che non sia necessario.