



# VAPT

VULNERABILITY ASSESSMENT  
AND PENETRATION TESTING REPORT

ANALISI CONDOTTA DA:  
LUIZA MELE

# ANALISI DELL'AZIENDA

L'azienda presa in Analisi è INVIA, compagnia basata in Australia, che si occupa di fornire soluzioni SaaS (Software as a Service) .

La particolarità del Software as a Service, sono applicazioni ospitate su Server remoti, fruibili dagli utenti da applicazione web.

INVIA vanta oltre 600 clienti tra aziende e enti governativi, con più di 500.000 endpoint gestiti. L'azienda si distingue per un tasso di fidelizzazione del 99% e il 90% del nuovo business proviene da referenze

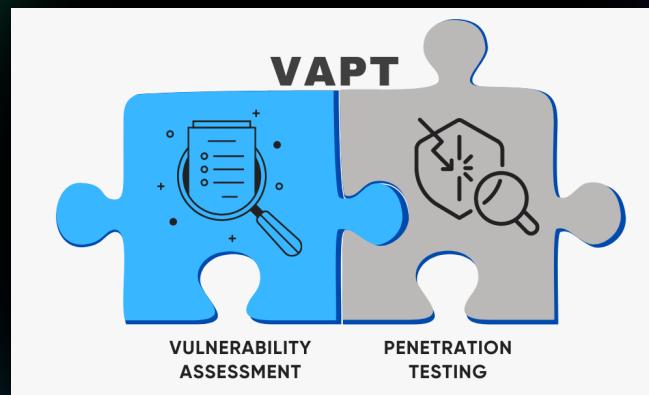


# IL VAPT

Il VAPT ha lo scopo di identificare e mitigare le vulnerabilità dei siti web e delle applicazioni.

Il VAPT è stato eseguito sull'azienda cliente ABC Pvt. Ltd., in data 04-06-2024, che ha ingaggiato INVIA per svolgere l'attività su una delle sue Web application.

Questo Vulnerability assessment e Penetration Testing è stato realizzato utilizzando gli standard OWASP, NIST e SANS, attraverso strumenti come Burp Suite, Nmap e Kali Linux.



# Gli ambiti su cui è stata basata la valutazione

---

L'ambito di questa valutazione ha incluso i seguenti test:

---

- Information Gathering
  - Configuration Management
  - Business Logic
  - Authentication
  - Authorization
  - Session Management
  - Data Validation, Governance, and Transfer.
-

#### Accounts

User	Role
J1@invia.co.in	Self-Register

#### Environment Details

Application Name	Demo
Environment	Production
Accessibility	INTERNET
Authentication Method	Login
Backend	AWS

# Metodologia

Per svolgere questo VAPT è stato utilizzato un account 'J1@invia.co.in', su un Environment di produzione, che fa relay su AWS (Amazon Web Services).

# Metodologia e strategia

Per evitare di impattare le attività dei clienti sono stati evitati i seguenti ambiti:

- Denial of Service (DoS) Attacks
- Brute Force Attacks
- Directory Fuzzing
- Exploits with Known Consequences
- Data Manipulation or Deletion
- Excessive Traffic Generation
- Unverified Third-Party Tools or Scripts
- Social Engineering Attacks
- Exhaustive Vulnerability Scanning
- Security Tests without Proper Authorization

# Classificazione delle vulnerabilità

Le vulnerabilità si dividono in diverse categorie in base alla loro severità ed impatto:

- **Critical**: sono vulnerabilità molto gravi che possono portare alla compromissione totale dell'applicazione;
- **High**: consentono attacchi mirati, come ad esempio Cross-Site-Scripting
- **Medium**: Sfruttate in combinazione con altre vulnerabilità riportano allo status 'High'.
- **Low**: sono vulnerabilità che non necessitano di una soluzione immediata, ma che non vanno trascurate.
- **Informational**: non sono direttamente sfruttabili dagli attaccanti, ma potrebbero essere utilizzate per scoprire delle informazioni.

# Vulnerabilità riscontrate

Le vulnerabilità riscontrate sono le seguenti:

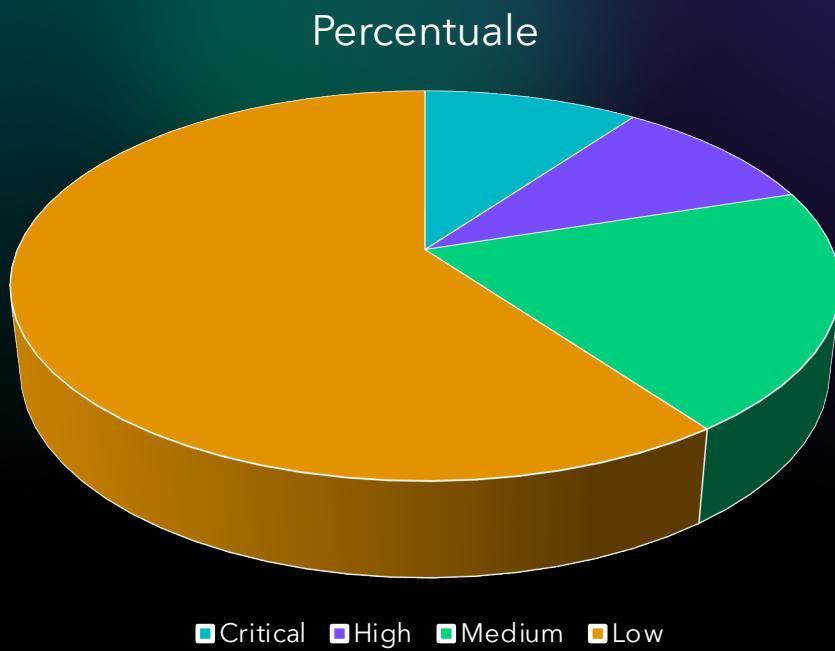
S. No.	Name	Severity	Risk Score	Status
1.	CSRF Leads to account takeover	Critical	9.1	Unresolved
2.	CSRF on the claim Create/ Update page	High	8.8	Unresolved
3.	Weak Password Policy (Password in plaintext)	Medium	6.5	Unresolved
4.	No Rate Limit	Medium	5.0	Unresolved
5.	Token doesn't implement properly (Token Misconfigured)	Low	3.1	Unresolved
6.	Outdated jQuery and Bootstrap	Low	3.1	Unresolved
7.	Clickjacking	Low	4.0	Unresolved
8.	Server Information Disclosed	Low	3.1	Unresolved
9.	HTTP Strict Transport Security (HSTS) Header is missing	Low	3.0	Unresolved
10.	CSP not implemented	Low	3.1	Unresolved

Facendo il conteggio abbiamo 1 vulnerabilità critica, 1 High, 2 Medium, 6 Low

# Percentuali delle vulnerabilità riscontrate

Le percentuali sono le seguenti:

- 10% Critical
- 10% High
- 20% Medium
- 60% Low



# CSRF

- **CVE** DI RIFERIMENTO: CVE-2023-33534
- **Remediation:**

Generare un token univoco e imprevedibile lato server per ogni richiesta autenticata.

Includere il token nei moduli e nelle richieste POST.

Il server deve verificare il token prima di elaborare la richiesta.

# CSRF nella Claim Create/Update page

- La CVE di riferimento è la stessa della precedente.

- **Remediation:**

Utilizzo di Token Anti-CSRF

Verifica degli Header HTTP

Evitare l'Uso di Metodi HTTP GET per Operazioni Sensibili

# Weak password policy

- CVE di riferimento: CWE-256: Plaintext Storage of a Password.

- **Remediation:**

Hashing delle Password

Uso di Salt Unici

Cifratura dei Dati Sensibili

Restrizione degli Accessi

# Outdated jQuery and Bootstrap

- L'utilizzo di versioni obsolete di jQuery e Bootstrap potrebbe esporre le applicazioni web a diverse vulnerabilità di sicurezza, in particolare attacchi come Cross-Site Scripting (XSS).
- CVEs di riferimento:
- JQuery:

**CVE-2020-11023:** Vulnerabilità, risolta nella versione 3.5.0 di jQuery.

- Bootstrap:

**CVE-2024-6484**

**CVE-2024-6485**

**CVE-2024-6531**

- **Remediation:**

- Aggiornamento alle Versioni Più Recenti
- Verifica delle dipendenze

# Clickjacking

CVE di riferimento

**CVE-2021-35237:** In Kiwi Syslog Server, assenza dell'header HTTP X-Frame-Options.

**CVE-2023-38873**

- **Remediation:**
- Impostazione dell'Header HTTP X-Frame-Options:

DENY: impedisce l'incorporamento da qualsiasi sorgente.

SAMEORIGIN: permette l'incorporamento solo da pagine dello stesso dominio.

- Utilizzo della Direttiva frame-ancestors della Content Security Policy (CSP).
- Implementazione di Framekiller tramite JavaScript: script che verifica se la pagina è caricata all'interno di un frame.

# Server Information Disclosed

- CVEs di riferimento:
- **CVE-2019-0704.**
- **CVE-2023-50315.**
- **Remediation:**
  - Configurazione del Server per Limitare le Informazioni Divulgate.
  - Personalizzazione delle Pagine di Errore.
  - Rimozione di File e Directory Non Necessari.

# HTTP Strict Transport Security (HSTS) Header is Missing

- CVEs di riferimento
- **CVE-2021-0296**
- **CVE-2021-38978**
- **CVE-2023-32762**

Remediation:

- includere l'header Strict-Transport-Security nelle risposte HTTPS.

# CSP Not Implemented

- CVEs di riferimento:
- **CVE-2018-5164**
- **CVE-2023-4324**

Remediation:

- Definire le Origini Consentite
- Utilizzare Nonce o Hash per Script Inline

Si consiglia di testare in Modalità Report-Only!

# Consigli utili

- Si consiglia di seguire i suggerimenti delle remediation riportate nel corrente Documento e di tenere aggiornate le librerie.
- Segnalare eventuali incidenti alle figure preposte e nei tempi preposti:

Il [d.l. 105/2019](#) (conv. con modifiche dalla L. 133/2019), approvato in condizioni di straordinaria necessità e urgenza provocate da attacchi che avevano interessato le reti di diversi Paesi europei, ha istituito il cd. “perimetro di sicurezza nazionale cibernetica” e impone **obblighi di notifica** degli “incidenti aventi impatto su reti, sistemi informativi e servizi informatici” in capo a enti **pubblici** e **privati** nazionali la cui operatività, correlandosi a **funzioni e servizi essenziali** per lo Stato, impatta sulla “**sicurezza nazionale**” (art. 1, commi 1 e 3, d.l. 105/2019).

- La **procedura** ideata per la segnalazione coinvolge una molteplicità di soggetti, gli enti sopra individuati devono, infatti, comunicare l’incidente al Computer Security Incident Response Team – **CSIRT** (in Italia istituito presso l’Agenzia per la cybersicurezza nazionale **ACN**), esso, a sua volta, inoltrerà tempestivamente la notizia al **Dipartimento delle informazioni per la sicurezza** il quale assicura poi la trasmissione delle notifiche ricevute all’organo del **Ministero dell’interno per la sicurezza e la regolarità dei servizi di telecomunicazione** nonché alla **Presidenza del Consiglio** dei ministri (se provenienti da un soggetto pubblico o da un soggetto di cui all’art. 29 [d.lgs. 82/2005](#)) ovvero al **Ministero dello sviluppo economico** (se effettuate da un soggetto privato).

Stando al testo del decreto n. 105/2009 il mancato adempimento dei doveri di comunicazione è punito, salvo che il fatto non costituisca reato, con la **sanzione amministrativa** pecuniaria da 250.000 euro a 1.500.000 euro (art. 1, comma 9, d.l. 105/2019).

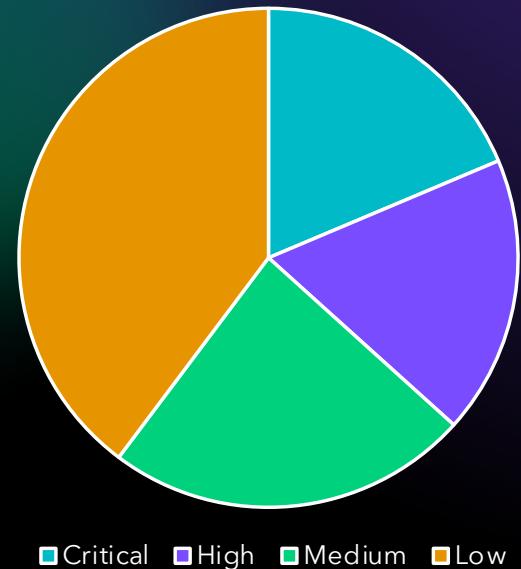
Al decreto legge è stata data attuazione con diversi atti normativi secondari, in particolare è il [DPCM n. 81/2021](#) a **regolamentare le notifiche degli incidenti** poc’anzi menzionati, definendo, in particolare, la “tassonomia degli incidenti” suddivisi per classe di gravità (art. 2), la procedura di inoltro delle segnalazioni (art. 5), le misure tecniche di sicurezza da adottare in caso di incidente (artt. 8 ss.).

FONTE: <https://www.compliancehub.it/2024/03/14/incidenti-informatici-cyber-attack-obblighi-di-segnalazione-megi-trashaj/>

# Risk score

S. No.	Name	Severity	Risk Score	Status
1.	CSRF Leads to account takeover	Critical	9.1	Unresolved
2.	CSRF on the claim Create/ Update page	High	8.8	Unresolved
3.	Weak Password Policy (Password in plaintext)	Medium	6.5	Unresolved
4.	No Rate Limit	Medium	5.0	Unresolved
5.	Token doesn't implement properly (Token Misconfigured)	Low	3.1	Unresolved
6.	Outdated jQuery and Bootstrap	Low	3.1	Unresolved
7.	Clickjacking	Low	4.0	Unresolved
8.	Server Information Disclosed	Low	3.1	Unresolved
9.	HTTP Strict Transport Security (HSTS) Header is missing	Low	3.0	Unresolved
10.	CSP not implemented	Low	3.1	Unresolved

Risk Percentage



# Costi

- Se consideriamo un costo medio di 400€ al giorno per persona, il numero di giorni lavorativi necessari per mitigare tutte le vulnerabilità è di 4,4 giorni.

Costo totale: 14.080€

- Considerando un team composto da 8 persone con uno stipendio mensile di 2500€ a persona. Il costo totale del team per un mese è 20.000€.

# Costi per attività

- Vulnerabilità Critica (CSRF - Account Takeover)

Tempo stimato: 1,5 giorni

Costo stimato: 4.800€

- Vulnerabilità Alta (CSRF - Claim Update Page)

Tempo stimato: 1,2 giorni

Costo stimato: 3.840€

- Vulnerabilità Medie (Weak Password Policy, No Rate Limit)

Tempo stimato: 1,0 giorni

Costo stimato: 3.200€

- Vulnerabilità Basse (Clickjacking, Outdated jQuery, Server Info Disclosure, HSTS Missing, CSP Not Implemented, Token Misconfigured)

Tempo stimato: 0,7 giorni

Costo stimato: 2.240€

# Vulnerabilità più comuni e recenti

- CVE-2025-22467: Vulnerabilità di overflow del buffer nello stack, che consente l'esecuzione di codice remoto da parte di un aggressore autenticato con privilegi limitati.

Fonte: <https://www.redhotcyber.com/post/ivanti-nel-mirino-la-vulnerabilita-con-cvss-9-9-potrebbe-essere-sfruttata-a-breve>

- CVE-2025-23114: Falla critica nel software di backup, che potrebbe permettere a un attaccante di eseguire codice arbitrario tramite un attacco "Man-in-the-Middle».

Fonte: <https://www.integrity360.com/it/en-us/resources/threat-intel-roundup/threat-intel-roundup-7-2-25>

- CVE-2025-21293: Una vulnerabilità di escalation dei privilegi in Active Directory, sfruttabile per ottenere accesso a livello di sistema all'interno di un ambiente Active Directory.

Fonte: <https://profect.it/vulnerabilita/exploit-cve-2025-21293-active-directory>

- Zero-day in Microsoft (febbraio 2025): Nel Patch Tuesday di febbraio 2025, Microsoft ha corretto quattro vulnerabilità zero-day, di cui due già attivamente sfruttate in rete.

- Fonte: <https://www.cybersecurity360.it/nuove-minacce/un-patch-tuesday-leggero-quello-di-febbraio-2025-ma-con-quattro-zero-day-corrette>

Grazie!