

Vulnerability Assessment Report

NetSpectres Academy

Redatto da: Riccardo Droghetti

Data: 7 giugno 2025

1. Pianificazione e Metodologia

L'applicazione analizzata è NetSpectres Academy, una piattaforma di formazione sulla cybersecurity, sviluppata in React e TypeScript.

È una SPA frontend-only testata in ambiente locale (porta 5173).

Tecnologie utilizzate:

- React (TSX), TypeScript, CSS
- Librerie: Framer Motion, Lucide Icons
- Ambiente: Localhost, frontend senza backend

Strumenti utilizzati:

- Manual Testing (Browser, DevTools)
- Nmap (localhost): Porta 5173 chiusa
- Nikto: Nessun header di sicurezza rilevato
- WhatWeb: Rilevato React
- Burp Suite (analisi richieste HTTP)

Approccio:

Grey Box - Codice frontend disponibile, test eseguiti con accesso utente.

2. Vulnerabilità Identificate

- Mancanza di Protezione Contro Brute Force sul Login

Il login non limita i tentativi falliti.	Nessun CAPTCHA, blocco o delay. CVSS 7.5 (High).
Impatto:	compromissione account tramite brute-force.
Soluzione:	CAPTCHA, blocco IP dopo tentativi falliti.

- Assenza di HTTPS

Il traffico	viaggia in chiaro. CVSS 6.1 (Medium).
Impatto:	intercettazione credenziali.
Soluzione:	utilizzare HTTPS e certificati TLS.

- Cookie non sicuri

Assenza di flag HttpOnly/Secure.	CVSS 6.5 (Medium).
Impatto:	session hijacking.
Soluzione:	impostare cookie sicuri e timeout sessioni.

- Assenza 2FA

Nessuna autenticazione a due fattori.	CVSS 5.0 (Medium).
Impatto:	rischio accesso abusivo.
Soluzione:	integrare Two-Factor Authentication.

- Leaderboard espone nomi utente

Visibilità pubblica dei nomi reali.	CVSS 4.3 (Medium).
Impatto:	social engineering.
Soluzione:	anonimizzare i nomi utente.

- Reset password mancante

Nessuna funzione per recuperare la password.	CVSS 5.3 (Medium).
Impatto:	perdita accesso.
Soluzione:	sistema di reset via email.

- Creazione moduli illimitata e senza moderazione

Moduli offensivi o duplicati permessi. CVSS 6.0 (Medium).

Soluzione: filtri contenuti, approvazione admin.

- Registrazione senza verifica email

Account infiniti creati senza controllo.

CVSS 6.5 (Medium).

Soluzione: email obbligatoria con verifica.

- XP Farming via Module Spam

Nessun limite XP per modulo → possibilità di abusarne. (Medium)

- Parole offensive non filtrate

Input senza restrizioni.

CVSS 4.0 (Low).

Impatto: contenuti inappropriati.

Soluzione: filtri anti-volgarità.

- Bug UI su click multipli

Blocchi navigazione causati da clic ripetuti.

CVSS 3.5 (Low).

Soluzione: debounce su navigazione

- Admin Username in Leaderboard

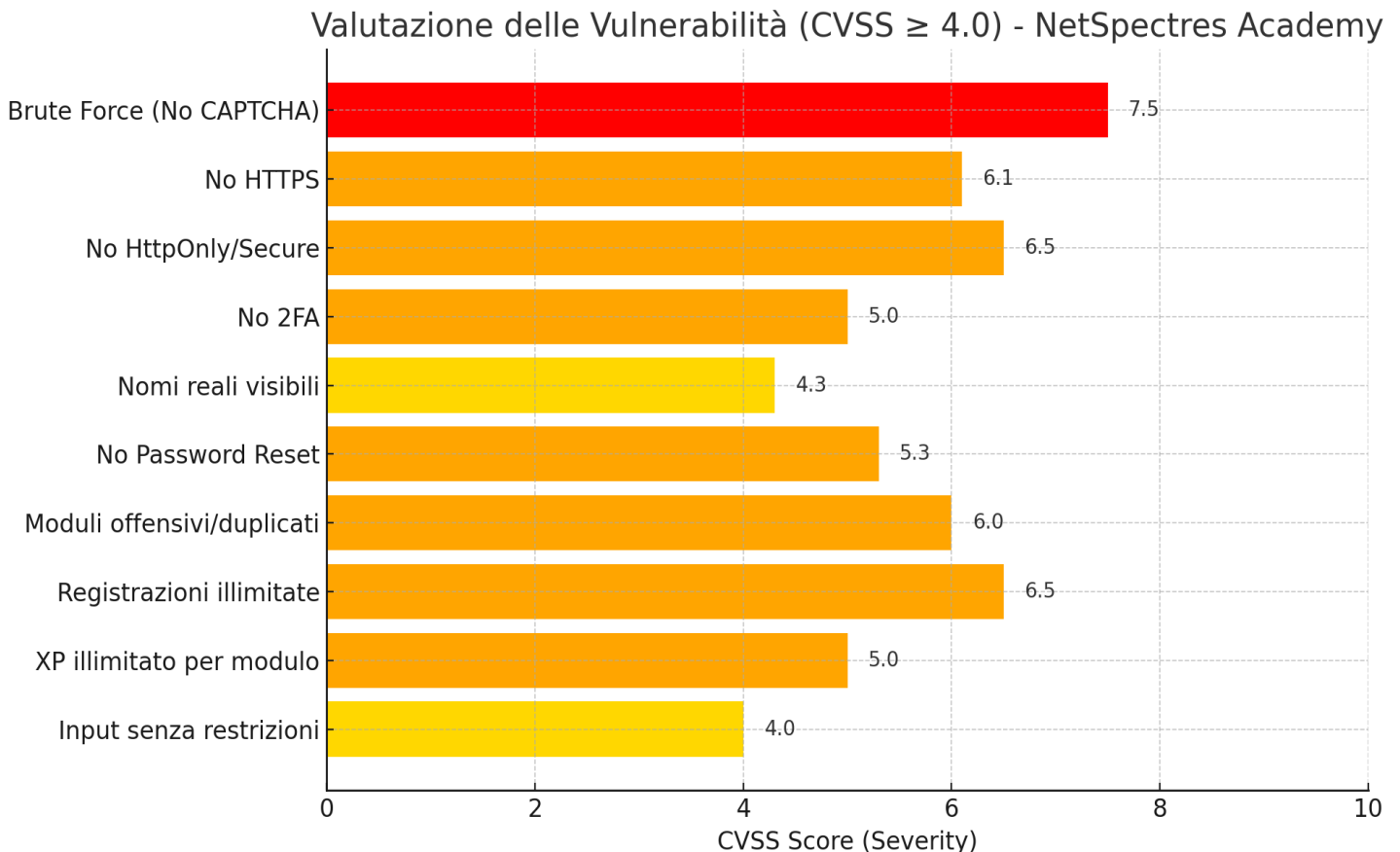
Presenza visibile dell'utente "admin". (Low)



Grafico a Barre Orizzontali — Gravità delle Vulnerabilità

Descrizione:

Questo grafico visualizza le vulnerabilità identificate in NetSpectres Academy, ordinate per nome e classificate in base al punteggio **CVSS** (Common Vulnerability Scoring System).



Didascalie:

- **Rosso (CVSS \geq 7.0):** Vulnerabilità ad alta gravità, da risolvere immediatamente.
- **Arancione (CVSS 5.0–6.9):** Rischi significativi, da gestire con priorità.
- **Giallo (CVSS 4.0–4.9):** Problemi di sicurezza minori ma comunque rilevanti.

Obiettivo del grafico:

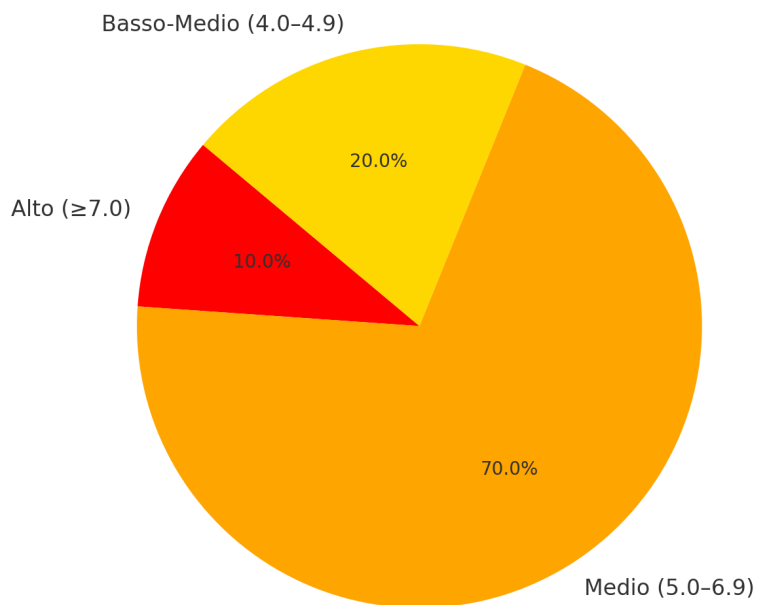
Evidenziare in modo chiaro **quali problemi di sicurezza hanno maggiore impatto** sull'integrità e la protezione dell'applicazione.

Grafico a Torta — Distribuzione delle Vulnerabilità per Severità

Descrizione:

Il grafico mostra la distribuzione percentuale delle vulnerabilità per fasce di gravità (escludendo i problemi a basso rischio).

Distribuzione delle Vulnerabilità (CVSS ≥ 4.0)



Didascalie:

- **Alto:** Percentuale di problemi critici (es. brute force, cookie insicuri).
- **Medio:** Vulnerabilità che possono causare danni moderati (es. 2FA mancante, reset password assente).
- **Basso-Medio:** Problemi minori che comunque meritano attenzione.

Obiettivo del grafico:

Fornire una **visione d'insieme immediata** su dove si concentra il rischio, facilitando la pianificazione delle azioni correttive.


3. Raccomandazioni Generali

Abilitare HTTPS con certificati SSL/TLS.

- Implementare meccanismi anti-brute force (CAPTCHA, rate-limiting).
- Usare cookie sicuri (`HttpOnly`, `Secure`, `SameSite`).
- Aggiungere Two-Factor Authentication (2FA).
- Limitare/moderare la creazione di moduli.
- Implementare password reset sicuro via email.
- Verifica email obbligatoria in fase di registrazione.
- Introdurre limiti XP per ridurre il farming.
- Risolvere i bug grafici, migliorando UX/accessibilità.

4. Funzionalità Mancanti e Conformità Legale

Elemento Mancante	Note
Privacy Policy	Obbligatoria per GDPR
Termini e condizioni	Necessari per uso regolare
Gestione consenso cookie (banner)	Assente, viola linee guida GDPR
Password recovery	Funzionalità assente
Login via provider esterni (Google, Facebook)	Non disponibile
Sezione Aiuto / Supporto	Non presente
Informazioni sul gestore / contatti	Nessuna trasparenza sul titolare
Funzionalità multilingua	Solo lingua italiana o inglese non specificata

 **Nota:** Queste funzionalità sono fondamentali per rispetto della normativa vigente e per una user experience professionale.

5. Output Tecnici

- Nmap: Comando: `nmap -p 5173 localhost`

Risultato: 5173/tcp closed

- Nikto:

Comando: `nikto -h http://localhost:5173`

Risultato: 0 host(s) tested

- WhatWeb:

Framework rilevato: React

Hosting: ambiente di sviluppo locale (es. Vite)

6. Conclusione

Conclusione

NetSpectres Academy si presenta come una piattaforma promettente nell'ambito della formazione alla cybersecurity, ma l'analisi ha evidenziato una serie di vulnerabilità che necessitano di interventi mirati e prioritari per garantire un livello di sicurezza adeguato agli standard attuali.

In particolare, è fondamentale potenziare il sistema di autenticazione degli utenti mediante l'introduzione di meccanismi come la **Two-Factor Authentication (2FA)**, accompagnata da ulteriori contromisure quali il **rate limiting**, la presenza di **CAPTCHA** e un sistema di recupero sicuro delle credenziali. Questi accorgimenti riducono in modo significativo il rischio di compromissione degli account da parte di attaccanti.

Parallelamente, è necessario intervenire sulla **protezione dei contenuti**, attivando header HTTP sicuri (come **Content-Security-Policy**, **X-Frame-Options** e **Strict-Transport-Security**) e implementando filtri efficaci contro contenuti offensivi o duplicati, prevenendo così abusi e manipolazioni all'interno della piattaforma.

Infine, per garantire la **riservatezza delle comunicazioni** e la conformità alle normative, è indispensabile adottare il protocollo **HTTPS** tramite l'ottenimento di un **certificato TLS** valido. Questo assicura che i dati scambiati tra l'utente e l'applicazione siano cifrati e protetti da intercettazioni.

L'integrazione di queste misure contribuirà a rafforzare la sicurezza complessiva della piattaforma, aumentando la fiducia degli utenti e garantendo una user experience più professionale e conforme alle buone pratiche del settore.

