CyberLens Vulnerability AI Scanner

Security Report

Blue Team AI Platform · v1.6.5 · 15/04/2026 16:30

Target	demo.cyberlens.it
IP	93.184.216.34
Scansione	2026-04-15 14:22
Report	15/04/2026 16:30
WAF	Cloudfront
SSL/TLS	TLSv1.2, TLSv1.3 ✓ · Issuer: Amazon/CN=Amazon RSA 2048 M02 · Scade in 312gg
Tecnologie	Amazon CloudFront, Nginx
Fonti dati	SpiderFoot OSINT · Nmap · Nikto · OWASP ZAP (9 finding unici) · Wappalyzer (Nginx, Amazon CloudFront)
Cliente	Organizzazione S.r.l. — DEMO

40/100

Grade B — BASSO

Indice di Rischio · 0-20 Molto Basso 21-40 Basso 41-70 Medio 71-85 Significante 86-100 Critico

Componente	Contributo	Dettaglio
CVE & Vulnerabilità	**+12.8 / 35**	3 CVE
Kill Chain Coverage	**+5.2 / 25**	MITRE ATT&CK;
Configurazione HTTP	**+20.0 / 20**	Header mancanti
Esposizione	**+2.0 / 20**	Porte/threat intel

3	0	0	3	3/14	8
CVE totali	Urgenza immediata	Exploit pubblici	Entro 30 giorni	Kill chain fasi	Misure D3FEND

DOCUMENTO DI ESEMPIO — Dati fittizi a scopo dimostrativo. Non si riferiscono a sistemi reali. Cliente demo: Organizzazione S.r.l.

Executive Summary

Sintesi Esecutiva

Stato di Sicurezza

L'ambiente **demo.cyberlens.it** (93.184.216.34) presenta un profilo di rischio moderato (**Grade B, 40/100**). Non sono state identificate vulnerabilità critiche che richiedono intervento immediato, ma tre difetti di sicurezza (CVE) richiedono remediation entro 30 giorni. L'infrastruttura è gestita su AWS CloudFront e Nginx, con protezione WAF attivo—un elemento positivo che mitiga già parte degli attacchi di rete comuni.

Rischi Principali

• **Clickjacking e Data Exfiltration**: Assenza di X-Frame-Options consente di incorporare l'API in frame malevoli, rischiando il furto di sessioni utente e dati sensibili.

• **Downgrade SSL/TLS**: Mancanza di HSTS permette agli utenti di connettersi via HTTP non criptato, esponendoli ad attacchi man-in-the-middle su reti pubbliche.

• **Superficie Esposta**: Il doppio protocollo (HTTP+HTTPS) aumenta i vettori d'attacco e complica il monitoraggio di security compliance.

Azioni Raccomandate

1. **Entro 7 giorni**: Implementare X-Frame-Options: DENY su CloudFront Distribution. Operazione a basso rischio, nessun downtime. Verifica il funzionamento monitorando i log di CloudFront.
2. **Entro 7 giorni**: Abilitare HSTS con max-age=31536000 secondi. Forza tutti i browser a comunicare solo in HTTPS. Testare in staging prima di applicare a produzione.
3. **Entro 30 giorni**: Disabilitare completamente HTTP su CloudFront Distribution. Implementare redirect HTTP→HTTPS come misura transitoria se i client non possono essere aggiornati immediatamente.

Valutazione Complessiva

Lo staging environment dimostra una **postura di sicurezza baseline solida**: WAF attivo, infrastruttura AWS moderna, nessuna CVE critica. I gap individuati sono **configurazioni assenti, non falle di design**—il che significa risolvibili in pochi giorni con modifiche minori.
Punti di forza: CloudFront WAF, HTTPS disponibile, nessun ritardo critico.
Aree di miglioramento: Hardening dei security header (mancanti), enforcement dello stack HTTPS-only.
Raccomandazione finale: Completare le tre azioni entro 30 giorni per passare da Grade B a A. Successivamente, implementare una policy di security headers as-code per evitare regressioni in futuri deployment.

Score Commentary

Analisi Risk Score 40/100 (Grade B)

Perché questo punteggio?

Il sistema registra un profilo di rischio **basso ma non trascurabile** dovuto principalmente a configurazioni difensive carenti su un'infrastruttura altrimenti ben protetta (CloudFront + TLS 1.2/1.3). Le tre CVE identificate sono datate (2001-2007) e prive di exploit pubblici, ma indicano esposizioni legacy potenzialmente sfruttabili in 30 giorni.

Fattori dominanti

1. **Configurazione (+20pt peso massimo)**: Assenza di 13 security header critici (CSP, X-Frame-Options, HSTS, X-XSS-Protection). Questa è la vulnerabilità più grave—permette clickjacking, XSS e MITM.
2. **CVE legacy (+12.77pt)**: Tre vulnerabilità con EPSS elevato (CVE-2007-6750 al 81.7%), benché non immediatamente exploitabili, riducono il security posture.
3. **Kill Chain (Execution/Credential Access)**: I missing header espongono direttamente le fasi iniziali di attacco.

Azioni concrete (10-15pt riduzione)

• Implementare HSTS, CSP (frame-ancestors 'none'), X-Frame-Options: DENY in 48 ore—riduce ~8pt
• Verificare versioni effettive Nginx e aggiornare patch non applicate—riduce ~4pt
• Aggiungere X-Content-Type-Options: nosniff, X-XSS-Protection in response headers—riduce ~3pt
Verdict: Ambiente staging accettabile, ma remediation degli header è urgente prima di produzione.

SSL/TLS Analysis

Protocollo	Stato	Campo	Valore
SSLv2	Disabilitato	Issuer	/C=US/O=Amazon/CN=Amazon RSA 2048 M02
SSLv3	Disabilitato	Algoritmo	sha256WithRSAEncryption
TLSv1.0	Disabilitato	RSA Key	2048 bit
TLSv1.1	Disabilitato	Valido dal	Jan 13 00:00:00 2026 GMT
TLSv1.2	**Abilitato ✓**	Scade il	Feb 10 23:59:59 2027 GMT
TLSv1.3	**Abilitato ✓**	Scadenza	**312 giorni**

✓ Configurazione TLS ottimale: TLS 1.3 abilitato. Il server utilizza il protocollo più recente e sicuro.
Certificato RSA (2048 bit): forza crittografica Adeguata.
Emesso da Amazon (CA commerciale riconosciuta).
✓ Certificato valido per altri 312 giorni.
✓ Renegotiazione TLS non supportata: riduce la superficie di attacco contro DoS via renegotiation.

Top 5 Vulnerabilità — Analisi AI

#1 CVE-2007-6750 CVSS 5.0 EPSS 81.7% 30 GIORNI

Analisi CVE-2007-6750 - Contesto Target
Rischio reale NON urgente per questo target. CVE-2007-6750 colpisce Apache 1.x/2.x, mentre il target usa CloudFront (CDN AWS) + Nginx. Nginx non è affetto da questa vulnerabilità Apache-specifica.
Vettore Un attaccante invierebbe richieste HTTP incomplete e lente (Slowloris) per esaurire socket connessioni, causando denial of service. Inapplicabile: CloudFront ha timeout globali configurati.
Remediation Nessuna azione richiesta per questa CVE. Verifica invece che CloudFront abbia Origin Shield abilitato e che Nginx sia aggiornato agli ultimi patch. Configura WAF rules CloudFront per rate-limiting su connessioni lente.

#2 CVE-2001-0902 CVSS 7.5 EPSS 41.3% 30 GIORNI

Analisi CVE-2001-0902 - Contesto Target
Rischio reale Praticamente nullo per questo target. La CVE riguarda IIS 5.0 (rilasciato 2000, EOL 2015) e il target usa Nginx. Il rischio esiste solo se dietro CloudFront gira un'applicazione legacy su IIS 5.0 non aggiornato.
Vettore Un attaccante inietterebbe caratteri hex-encoded negli header HTTP per aggiungere righe false nei log, inquinando audit trail e mascherando attività malevole.
Remediation Verificare con il team infrastruttura che non vi siano istanze IIS legacy. Se confermata assenza di IIS: nessuna azione richiesta.

#3 CVE-2002-1745 CVSS 7.5 EPSS 10.2% 30 GIORNI

Analisi CVE-2002-1745 - Contesto Target
Rischio reale Rischio molto basso. La vulnerabilità riguarda IIS 5.0 e uno script sample obsoleto; CloudFront non espone direttamente IIS ed è improbabile che CodeBrws.asp sia in produzione.
Vettore Accesso diretto a /CodeBrws.asp per leggere il source code sfruttando l'off-by-one in estensioni.
Remediation 1. Verificare se CodeBrws.asp esiste nel documentRoot. 2. Se presente, eliminarlo. 3. Verificare log CloudFront ultimi 90 giorni per accessi anomali. PRIORITÀ 90_GIORNI.

Vulnerabilità Rilevate

CVE ID	CVSS	EPSS	Exploit	Urgenza	CWE
CVE-2007-6750	5.0	81.7%	—	30 GIORNI	CWE-399
CVE-2001-0902	7.5	41.3%	—	30 GIORNI	—
CVE-2002-1745	7.5	10.2%	—	30 GIORNI	CWE-193

Kill Chain — MITRE ATT&CK; Coverage

Stato	Fase	Rischio	Tecniche ATT&CK;
Assente	Reconnaissance	3/10	—
Assente	Resource Development	2/10	—
Assente	Initial Access	9/10	—
8/10	Execution	8/10	T1059.007
Assente	Persistence	6/10	—
Assente	Privilege Escalation	8/10	—
Assente	Defense Evasion	6/10	—
7/10	Credential Access	7/10	T1040
Assente	Discovery	4/10	—
Assente	Lateral Movement	9/10	—
6/10	Collection	6/10	T1557, T1185
Assente	Command and Control	7/10	—
Assente	Exfiltration	8/10	—
Assente	Impact	8/10	—

Contromisure D3FEND

ID	Contromisura	TTP	Implementazione
D3-CSP	Content Security Policy	8	CSP impedisce clickjacking (frame-ancestors 'none') e session hijacking
D3-XFO	X-Frame-Options Header	5	Impostare X-Frame-Options: DENY o SAMEORIGIN
D3-SC	Secure Cookie Attributes	5	Cookie con attributi Secure, HttpOnly, SameSite=Strict
D3-WAAF	Web Application Firewall	3	Regole WAF anti-XSS (OWASP ModSecurity CRS rule 941xxx)
D3-OTF	Output Encoding / Sanitization	3	Sanitizzare e fare encoding di tutti gli output HTML
D3-TLS	Transport Layer Security	1	TLS 1.3 obbligatorio, disabilitare SSL/TLS 1.0/1.1
D3-HSTS	HTTP Strict Transport Security	1	Abilitare HSTS con max-age >= 31536000 e includeSubDomains
D3-CVAL	Certificate Validation	1	Validazione rigorosa dei certificati TLS, HPKP o Certificate Transparency

Piano di Azione (POAM)

■ IMMEDIATA (3 azioni)

ID	Azione	Responsabile / Effort	Mitigazione
P01	Implementare X-Frame-Options: DENY su CloudFront Distribution	DevOps / Infra Lead · 30 min	Riduce rischio Execution (8/10→5/10). Custom Response Header in CloudFront: 'X-Frame-Options: DENY'
P02	Abilitare HSTS con max-age=31536000 su CloudFront	DevOps / Infra Lead · 20 min	Elimina vettore downgrade TLS. Header: 'Strict-Transport-Security: max-age=31536000; includeSubDomains'
P03	Verificare e disabilitare HTTP su CloudFront Distribution	DevOps / Infra Lead · 15 min	Impostare 'Viewer Protocol Policy' a 'HTTPS only'. Verifica con curl -I http://demo.cyberlens.it

■ 30 GIORNI (4 azioni)

ID	Azione	Responsabile / Effort	Mitigazione
P04	Implementare Content Security Policy (CSP) con frame-ancestors none e default-src self	AppSec / Backend · 4 ore	Header: 'Content-Security-Policy: default-src self; frame-ancestors none; style-src self unsafe-inline'. Testare con browser dev tools.
P05	Implementare X-Content-Type-Options: nosniff + X-XSS-Protection: 1; mode=block	DevOps / Infra Lead · 30 min	Custom Response Headers CloudFront: 'X-Content-Type-Options: nosniff' e 'X-XSS-Protection: 1; mode=block'
P06	Patch management su Nginx backend e validazione configurazione server	Infra / Linux Admin · 1 gg	Verificare 'nginx -v'. Se obsoleto pianificare upgrade. Aggiornare ssl_protocols per disabilitare TLS legacy.
P07	Configurare AWS WAF con OWASP ModSecurity CRS rules (941xxx per XSS)	Security / WAF Admin · 1 sprint	Abilitare AWS Managed Rules (AmazonIpReputationList, AWSManagedRulesCommonRuleSet). Rate limiting: 2000 req/5min.

■ 90 GIORNI (4 azioni)

ID	Azione	Responsabile / Effort	Mitigazione
P08	Implementare Secure Cookie Attributes (Secure, HttpOnly, SameSite=Strict)	AppSec / Backend · 2 gg	SetCookie con 'Secure; HttpOnly; SameSite=Strict; Path=/; Domain=.cyberlens.it'. Verifica con curl.
P09	Implementare Output Encoding / HTML Sanitization su tutti gli endpoint (D3-OTF)	AppSec / Backend · 1 sprint	Usare HtmlEncoder .NET, DOMPurify JS. Audit con Semgrep rule owasp.injection. Pen test post-implementazione.
P10	Implementare Referrer-Policy e Cross-Origin-Resource-Policy su CloudFront	DevOps / Infra Lead · 1 ora	Custom Response Headers: 'Cross-Origin-Resource-Policy: same-origin' e 'Referrer-Policy: strict-origin-when-cross-origin'
P11	Revisione architetturale e migrazione a stack LTS aggiornato	Architecture / CTO · 2 sprint	Roadmap: T1 assessment, T2 POC su stack aggiornato con CloudFront, T3 cut-over. Risk score atteso: 20-25/100.

Note Strategiche

Il risk score attuale (40/100, Grade B) è moderato ma stabilizzato su vulnerabilità legacy. Le tre CVE non hanno exploit pubblici attivi, ma la configurazione deficitaria degli security header (13 header mancanti) e la kill chain aperta su Execution (8/10) indicano postura difensiva fragile. Azioni immediate focalizzate su CloudFront header injection in 30 minuti ciascuna: riducono il rischio a 32/100 senza dependency dev.

I 30 giorni risolvono il debito configurativo (CSP, HSTS, WAF rules) con effort distribuito tra Infrastructure e AppSec. Questa fase è il nucleo della remediazione: riduce Execution a 6/10 e Collection a 4/10.

I 90 giorni affrontano hardening strutturale (cookie security, output encoding) e strategia architetturale. La revisione dello stack è raccomandazione di lungo termine; senza di essa, il risk score rimane ancorato a 25-30/100 per obsolescenza.

Next step: eseguire P01-P03 entro fine settimana, validare con nmap/nikto, bloccare produzione fino a P04-P07 completate. Timeline totale: 4 settimane a rischio controllato.

OWASP Top 10 2025 — ZAP Mapping

5/10	0	9	0	50%
Categorie rilevate	Critical / High	ZAP finding (tipi)	CVE mappate	Coverage

■ Critical/High ■ Medium ■ Low ■ Info ■ Assente

	OWASP ID	Categoria	Stato	Severità	ZAP	CVE
■	A01:2025	Broken Access Control	ASSENTE	—	0	0
■	A02:2025	Security Misconfiguration	RILEVATO	LOW	3	0
■	A03:2025	Software Supply Chain Failures	ASSENTE	—	0	0
■	A04:2025	Cryptographic Failures	RILEVATO	LOW	1	0
■	A05:2025	Injection	ASSENTE	—	0	0
■	A06:2025	Insecure Design	RILEVATO	MEDIUM	3	0
■	A07:2025	Authentication Failures	RILEVATO	INFO	1	0
■	A08:2025	Software or Data Integrity Failures	ASSENTE	—	0	0
■	A09:2025	Security Logging and Alerting Failures	RILEVATO	LOW	1	0
■	A10:2025	Mishandling of Exceptional Conditions	ASSENTE	—	0	0

Dettaglio Finding ZAP per Categoria

A02:2025 — Security Misconfiguration ZAP:3 CVE:0

Finding	Severità	Istanze	CWE	Soluzione
Cookie No HttpOnly Flag	LOW	2	CWE-1004	Ensure that the HttpOnly flag is set for all cookies.
Tech Detected - Amazon CloudFront	INFO	1	CWE--1	
Re-examine Cache-control Directives	INFO	2	CWE-525	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate".

A04:2025 — Cryptographic Failures ZAP:1 CVE:0

Finding	Severità	Istanze	CWE	Soluzione
Strict-Transport-Security Header Not Set	LOW	5	CWE-319	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.

A06:2025 — Insecure Design ZAP:3 CVE:0

Finding	Severità	Istanze	CWE	Soluzione
Content Security Policy (CSP) Header Not Set	MEDIUM	1	CWE-693	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
X-Content-Type-Options Header Missing	LOW	2	CWE-693	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.
User Agent Fuzzer	INFO	24	CWE-1021	

A07:2025 — Authentication Failures ZAP:1 CVE:0

Finding	Severità	Istanze	CWE	Soluzione

Session Management Response Identified	INFO	15	CWE--1	This is an informational alert rather than a vulnerability and so there is nothing to fix.

A09:2025 — Security Logging and Alerting Failures ZAP:1 CVE:0

Finding	Severità	Istanze	CWE	Soluzione
Big Redirect Detected (Potential Sensitive Information)	LOW	2	CWE-201	Ensure that no sensitive information is leaked via redirect responses.