Sergiu Vlad

SERGIUVLAD.COM

RAPORT DE EVALUARE A SECURITĂȚII

Evaluarea expunerii externe și a aplicației web

Brightvale Freight SRL (fictiv): prezența publică pe internet, serverul de e-mail și portalul pentru clienți app.example.com.

EXEMPLU — COMPANIE FICTIVĂ, CONSTATĂRI ILUSTRATIVE

Acest exemplu arată structura și nivelul de detaliu ale unui raport real. Compania, domeniile (RFC 2606), adresele IP (RFC 5737), dovezile și constatările sunt inventate, cu scop ilustrativ.

CLIENT Brightvale Freight SRL (fictiv)	SERVICIU Evaluarea vulnerabilităților
SCOP Verificarea expunerii externe + evaluarea vulnerabilităților aplicației web	PERIOADĂ 2026 (testare și retestare)
RAPORT SV-SAMPLE-2026-01, versiunea 1.1 (include retestarea)	CLASIFICARE Confidențial — exemplu

ÎNTOCMIT DE
Sergiu Vlad

me@sergiuvlad.com · sergiuvlad.com

01

Rezumat executiv

Ce s-a testat, ce s-a găsit și ce trebuie făcut mai întâi, pe limba afacerii.

Brightvale Freight a solicitat o evaluare a vulnerabilităților pentru prezența sa publică pe internet și pentru portalul destinat clienților, **app.example.com**. Testarea s-a desfășurat în 2026, pe baza unei autorizări semnate, într-un interval agreat și fără a perturba sistemele în funcțiune.

Am identificat **opt probleme**. Niciuna nu este critică, dar **două au risc ridicat** și trebuie remediate în câteva zile: un modul învechit pe site-ul public, care expune datele din solicitările clienților, și o pagină de autentificare pentru administrare la care parola poate fi ghicită fără limită. Ambele pot fi exploatate de un atacator fără informații din interior.

E-mailurile trimise în numele example.com pot fi în prezent imitate, ceea ce facilitează fraudele cu facturi false către clienți. Trei conturi ale companiei apar în date publice provenite din breșe de securitate. În limitele acestei evaluări nu au fost observate semne ale unei compromiteri active.

După retestare, **șase din cele opt constatări sunt remediate și verificate**. Celelalte două au responsabili și termene. Expunerea generală a scăzut de la **Crescută** la **Scăzută**.

EXPUNERE GENERALĂ — INIȚIAL

Crescută

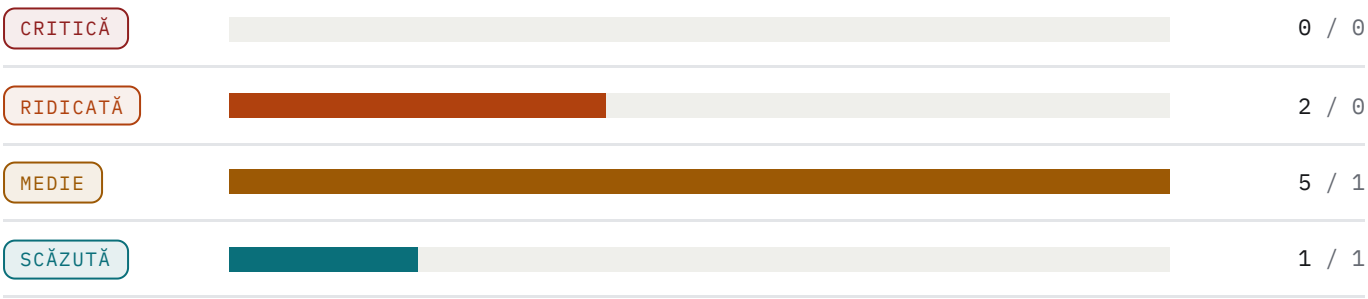
Două probleme cu risc ridicat, accesibile din internet fără credențiale.

EXPUNERE GENERALĂ — DUPĂ RETESTARE

Scăzută

Nu mai există probleme cu risc ridicat. Două puncte cu risc mai mic sunt planificate.

IMAGINEA RISCULUI (CONSTATĂRI PE SEVERITATE) — INIȚIAL / DESCHISE DUPĂ RETESTARE



Barele arată evaluarea inițială. Cifrele gri: constatări încă deschise după retestare.

PRIMELE TREI ACȚIUNI

01 **Actualizați modulul site-ului** semnalat la F-01 și eliminați modulele nefolosite.

02 **Protejați autentificarea de administrare** cu autentificare în doi pași, limitarea încercărilor și o listă de IP-uri permise.

03 **Finalizați autentificarea e-mailului**: semnați toate mesajele trimise (DKIM) și aplicați DMARC, astfel încât nimeni să nu poată trimite facturi în numele dumneavoastră.

02

Scop și metodologie

Au fost testate doar activele de mai jos, pe baza unei autorizări scrise. Orice element nelistat a fost în afara scopului.

ACTIVE INCLUSE ÎN SCOP

ACTIV	DESCRIERE	TESTARE
`example.com`, `www.example.com`	Site public (sistem de administrare a conținutului)	Verificare pasivă, evaluarea vulnerabilităților
`app.example.com`	Portal pentru clienți (aplicație web și API)	Evaluarea vulnerabilităților, autentificat cu două conturi de test (client, dispecer)
`mail.example.com`	Server de e-mail (SMTP, IMAP)	Verificare pasivă, analiza TLS
`staging.example.com`	Descoperit în etapa de recunoaștere; inclus în scop de client, în scris	Evaluarea vulnerabilităților
`203.0.113.0/28`	Interval de IP-uri publice, 16 adrese	Analiza serviciilor externe

În afara scopului: rețeaua internă, personalul (fără phishing), atacurile de tip denial-of-service, accesul fizic și serviciile terților, cu excepția înregistrărilor DNS și de e-mail.

CUM S-A DESFĂȘURAT LUCRAREA

01	**Autorizare**	Autorizare semnată și reguli de desfășurare (ref. AUTH-SAMPLE-2026-01): active, interval de testare, persoane de contact, condiții de oprire.
02	**Recunoaștere pasivă**	DNS public, jurnale de transparență a certificatelor, motoare de căutare și indexuri publice de breșe. Niciun trafic trimis către sistemele clientului.
03	**Evaluare**	Scanare și analiză asistate de AI; fiecare constatare validată manual. OWASP WSTG pentru site și portal. Fără teste distructive, fără denial-of-service.
04	**Clasificare**	Scor de bază CVSS v3.1, ajustat la contextul afacerii. Corelat cu MITRE ATT&CK acolo unde este relevant.
05	**Raport și retestare**	Prezentarea rezultatelor echipei clientului, apoi retestarea fiecărei remedieri. Această versiune (1.1) include rezultatele retestării.

STANDARDE

`OWASP WSTG v4.2` `PTES` `CVSS v3.1` `MITRE ATT&CK v20.1` `OWASP Top 10:2025`

03

Constatări

Ordonate după severitate. Dovezile sunt prescurtate și anonimizate; dovezile complete rămân la echipa clientului.

F-01

RIDICATĂ

Modul învechit pe site, cu o vulnerabilitate cunoscută public

CVSS V3.1 7,5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N ACTIV www.example.com

REFERINȚĂ OWASP Top 10:2025 A03 · ATT&CK T1190

CE AM GĂSIT

Modulul pentru formularul de contact (numele este omis în acest exemplu) rulează versiunea 3.2.1. Versiunea este afectată de o vulnerabilitate cunoscută, listată în avertismente publice: injecție SQL fără autentificare, remediată de producător în 3.2.4.

IMPACT ASUPRA AFACERII

Un atacator ar putea citi baza de date a site-ului, inclusiv solicitările clienților (nume, telefoane, detalii de transport). Ar fi o încălcare a securității datelor personale conform GDPR, cu obligații de notificare.

RETESTARE REMEDIAT

Versiunea 3.2.5 confirmată; cererea de test nu mai este întârziată. Două module nefolosite eliminate.

DOVEZI · ILUSTRATIVE, ANONIMIZATE

```
GET /plugins/[redacted]/readme.txt
HTTP/1.1 200 OK
Stable tag: 3.2.1

POST /forms/submit (test bazat pe timp, 1 cerere)
-> răspuns întârziat 5,0 s; nicio dată extrasă
```

REMEDIERE

- Actualizați modulul la 3.2.4 sau mai nou; activați actualizările automate de securitate.
- Eliminați modulele instalate, dar nefolosite.
- Verificați jurnalele serverului web pentru încercări anterioare de exploatare.

F-02

RIDICATĂ

Autentificare de administrare expusă, fără doi pași și fără limitarea încercărilor

CVSS V3.1 7,4 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N ACTIV www.example.com/admin/

REFERINȚĂ WSTG-ATHN-03 · ATT&CK T1110

CE AM GĂSIT

Pagina de autentificare pentru administrarea site-ului este accesibilă de la orice adresă IP. Permite încercări nelimitate de parolă, fără CAPTCHA sau întârziere, și nu cere un al doilea factor.

IMPACT ASUPRA AFACERII

O parolă ghicită sau refolosită oferă control total asupra site-ului public: modificarea paginilor, descărcări malițioase pentru vizitatori sau o pagină de plată falsă sub marca dumneavoastră.

RETESTARE REMEDIAT

Doi pași activi pentru 4 conturi de administrator; /admin/ răspunde 403 din afara listei permise.

DOVEZI · ILUSTRATIVE, ANONIMIZATE

```
POST /admin/login × 50 în 60 s (parolă greșită,
cont de test)
-> 50 × HTTP 200 "Invalid credentials"
-> fără blocare, fără întârziere, fără MFA
```

REMEDIERE

- Activați autentificarea în doi pași pentru toate conturile de administrator.
- Limitați încercările și blocați temporar după eșecuri repetate.
- Restricționați /admin/ la IP-ul biroului sau la VPN.

F-03

MEDIE

SSH deschis spre internet, cu autentificare prin parolă

CVSS V3.1 6,5 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N ACTIV 203.0.113.10:22 REFERINȚĂ ATT&CK T1133 · T1110.001

CE AM GĂSIT

Serverul 203.0.113.10 acceptă autentificare SSH cu parolă de la orice adresă IP. Încercările automate de ghicire a parolelor împotriva acestor servere sunt permanente pe internet.

IMPACT ASUPRA AFACERII

O singură parolă slabă sau refolosită i-ar oferi unui atacator acces pe serverul care găzduiește mediul de test și copiile de siguranță zilnice.

RETESTARE REMEDIAT

Este oferită doar autentificarea cu chei; portul 22 este filtrat din afara listei permise.

DOVEZI · ILUSTRATIVE, ANONIMIZATE

```
$ ssh -v [redacted]@203.0.113.10
debug1: Authentications that can continue:
        publickey,password
```

REMEDIERE

- Permiteți doar autentificarea cu chei (PasswordAuthentication no).
- Limitați portul 22 la VPN sau la IP-urile cunoscute ale administratorilor.

F-04

MEDIE

Versiuni TLS învechite și cifruri slabe pe serverul de e-mail

CVSS V3.1 Fără scor (context) ACTIV mail.example.com:443, :587, :993 REFERINȚĂ WSTG-CRYP-01

CE AM GĂSIT

Serverul de e-mail acceptă încă TLS 1.0 și TLS 1.1 și oferă suite de cifruri vechi (3DES, CBC cu SHA-1). Recomandarea actuală este TLS 1.2 sau mai nou, cu cifruri moderne.

IMPACT ASUPRA AFACERII

Slăbește protecția e-mailurilor și a parolelor în tranzit și nu trece verificările din multe chestionare de securitate ale clienților și ale asigurătorilor.

RETESTARE REMEDIAT

Sunt oferite doar TLS 1.2 și 1.3; niciun cifru vechi.

DOVEZI · ILUSTRATIVE, ANONIMIZATE

```
TLS 1.0   offered (deprecated)
TLS 1.1   offered (deprecated)
TLS_RSA_WITH_3DES_EDE_CBC_SHA   offered
```

REMEDIERE

- Dezactivați TLS 1.0 și 1.1; păstrați TLS 1.2 și 1.3.
- Folosiți un profil modern de cifruri (forward secrecy, doar cifruri AEAD).

F-05

MEDIE

Listarea directoarelor pe subdomeniul de test

CVSS V3.1 5,3 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N ACTIV staging.example.com/builds/ REFERINȚĂ WSTG-CONF-04

CE AM GĂSIT

Mediul de test este public și afișează conținutul directorului /builds/: arhive vechi ale versiunilor și un fișier de configurare exemplu care dezvăluie nume de servere interne și tehnologiile folosite.

IMPACT ASUPRA AFACERII

Îi oferă unui atacator o hartă a sistemelor interne și cod vechi de studiat. Mediile de test sunt adesea mai puțin actualizate decât producția.

RETESTARE REMEDIAT

staging.example.com cere acum autentificare; /builds/ răspunde 401.

DOVEZI · ILUSTRATIVE, ANONIMIZATE

```
GET https://staging.example.com/builds/
HTTP/1.1 200 OK
<title>Index of /builds</title>
  release-2026-[redacted].tar.gz
  .env.example
```

REMEDIERE

- Dezactivați listarea directoarelor pe serverul web.
- Puneți mediul de test în spatele autentificării sau al VPN-ului; ștergeți arhivele vechi.

F-06

MEDIE

Conturi ale companiei prezente în date publice din breșe

CVSS V3.1 Fără scor (context) ACTIV conturi @example.com REFERINȚĂ ATT&CK T1078

CE AM GĂSIT

3 conturi din domeniul example.com apar în 2 seturi publice de date provenite din breșe ale unor servicii terțe. Sunt raportate doar conturile afectate și numărul lor; parolele nu au fost colectate și nici consultate.

IMPACT ASUPRA AFACERII

Dacă angajații au refolosit acele parole la serviciu, un atacator s-ar putea autentifica în e-mail sau în portal ca utilizator legitim.

RETESTARE REMEDIAT

Resetarea parolelor confirmată de client; solicitarea celui de-al doilea factor verificată la autentificarea în webmail pentru cele 3 conturi.

DOVEZI · ILUSTRATIVE, ANONIMIZATE

```
a[redacted]@example.com   2 seturi
o[redacted]@example.com   1 set
s[redacted]@example.com   1 set
```

REMEDIERE

- Resetați parolele celor 3 conturi; impuneți doi pași pentru e-mail.
- Activați verificarea parolelor noi față de listele de parole compromise.

F-07

MEDIE

E-mailul poate fi falsificat: DMARC neaplicat, DKIM lipsă pentru un expeditor

CVSS V3.1 Fără scor (context) ACTIV example.com (DNS) REFERINȚĂ Autentificarea e-mailului · ATT&CK T1566

CE AM GĂSIT

Politica DMARC este p=none (doar monitorizare), iar serviciul de facturare care trimite în numele example.com nu semnează cu DKIM. Serverele destinatare nu sunt instruite să respingă mesajele falsificate.

IMPACT ASUPRA AFACERII

Infractorii pot trimite clienților dumneavoastră facturi false convingătoare, cu alte date bancare, de pe domeniul dumneavoastră real.

RETESTARE ÎN CURS

DKIM activ pentru toți expeditorii; DMARC la p=quarantine. p=reject planificat după 4 săptămâni de rapoarte curate.

DOVEZI · ILUSTRATIVE, ANONIMIZATE

```
$ dig +short TXT _dmarc.example.com
"v=DMARC1; p=none; rua=mailto:dmarc@example.com"
$ dig +short TXT [redacted]._domainkey.example.com
(nicio înregistrare)
```

REMEDIERE

- Activați DKIM pentru fiecare serviciu care trimite ca example.com.
- Treceți DMARC la p=quarantine, apoi la p=reject după analiza rapoartelor.

F-08

SCĂZUTĂ

Antete de securitate lipsă pe portalul pentru clienți

CVSS V3.1 Fără scor (context) ACTIV app.example.com REFERINȚĂ WSTG-CONF-07 · OWASP Secure Headers Project

CE AM GĂSIT

Răspunsurile nu conțin antetele Content-Security-Policy și Strict-Transport-Security și nici o regulă frame-ancestors. Nu a fost găsită o problemă exploatabilă, dar aceste antete limitează efectele unor eventuale erori viitoare.

IMPACT ASUPRA AFACERII

Apărare în profunzime: fără aceste antete, o eventuală vulnerabilitate de tip cross-site scripting sau o încercare de clickjacking are mai multe șanse de reușită.

RETESTARE PLANIFICAT

Planificat pentru următoarea versiune a portalului; va fi confirmat la cerere sau la o verificare trimestrială.

DOVEZI · ILUSTRATIVE, ANONIMIZATE

```
HTTP/2 200
content-type: text/html; charset=utf-8
(fără content-security-policy)
(fără strict-transport-security)
```

REMEDIERE

- Adăugați HSTS și frame-ancestors 'none'.
- Introduceți Content-Security-Policy în modul report-only, apoi aplicați-o.

04

Plan de remediere

Prioritizat după risc și efort. Efortul este o estimare pentru echipa clientului; pot face și eu partea practică, la cerere, cu ofertă separată.

CONSTATARE	ACȚIUNE	EFORT	RESPONSABIL
ACUM — ÎN 7 ZILE			
F-01	Actualizarea modulului, eliminarea celor nefolosite, verificarea jurnalelor	1–2 ore	Agenția web
F-02	Doi pași pentru administratori, limitarea încercărilor, listă de IP-uri permise	2–4 ore	Agenția web
F-06	Resetarea a 3 parole, doi pași obligatorii pentru e-mail	1 oră	IT
URMĂTORUL PAS — ÎN 30 DE ZILE			
F-03	SSH doar cu chei, restricționarea portului 22	1 oră	IT
F-04	Dezactivarea TLS 1.0/1.1 și a cifrurilor vechi	1–2 ore	IT
F-05	Dezactivarea listării, mediul de test în spatele autentificării	1 oră	Agenția web
F-07	DKIM pentru toți expeditorii, DMARC p=quarantine	2 ore	IT
ULTERIOR — ÎN 90 DE ZILE			
F-07	DMARC p=reject după analiza rapoartelor	30 min	IT
F-08	HSTS, frame-ancestors, CSP (întâi report-only)	0,5–1 zi	Echipa portalului
–	Recomandat: verificare externă trimestrială pentru expuneri noi (pachetul Protect)	Recurent	Decizia clientului

05

Rezultatele retestării

Fiecare remediere a fost verificată din nou, cu aceeași metodă ca la constatarea inițială. Raportul se încheie cu dovezi, nu cu promisiuni.

6	1	1
REMEDIATE ȘI VERIFICATE	ÎN CURS	PLANIFICATE
F-01, F-02, F-03, F-04, F-05, F-06	F-07	F-08

Risc rezidual după retestare: Scăzut. Nu mai există nicio problemă deschisă cu risc ridicat. F-07 este remediată parțial (DKIM activ, DMARC la p=quarantine) și trece la p=reject după patru săptămâni de rapoarte curate; F-08 intră în următoarea versiune a portalului. Ambele pot fi confirmate la cerere sau la o verificare trimestrială.

06

Anexă

A. METODA DE CLASIFICARE

Severitatea urmează scorul de bază CVSS v3.1: **Critică** 9,0–10,0, **Ridicată** 7,0–8,9, **Medie** 4,0–6,9, **Scăzută** 0,1–3,9. Scorul este apoi interpretat în contextul afacerii (datele implicate, expunerea, ușurința exploatării).

Constatările fără o cale tehnică de exploatare concretă (conturile din date publice din breșe, autentificarea e-mailului, securitatea transportului și antetele de protecție) sunt clasificate după context, nu printr-un vector CVSS, și marcate „fără scor”: nivelul este decis de accesibilitatea din internet și de ce ar obține un atacator.

B. AUTORIZARE

Toate testele au fost efectuate pe baza unei autorizări scrise, semnate de un reprezentant împuternicit al clientului (ref. AUTH-SAMPLE-2026-01), doar pentru activele din secțiunea 02 și în intervalul agreat. Clientul a confirmat că deține sau controlează fiecare activ.

C. CONFIDENȚIALITATE

Acest raport este confidențial și destinat clientului. Constatările, dovezile și orice date întâlnite sunt tratate conform unui acord de confidențialitate (NDA) și stocate criptat. Dovezile brute se șterg la 30 de zile după raportul final; raportul și autorizarea semnată se păstrează 12 luni ca evidență a proiectului, apoi se șterg sau se returnează, după preferința clientului.

Parolele din datele publice din breșe nu sunt niciodată colectate sau raportate: doar conturile afectate și numărul lor.

D. LIMITĂRI

Rezultatele reflectă starea sistemelor din scop în intervalul de testare. O evaluare reduce riscul și documentează diligența; **nu poate garanta că sistemele nu vor fi niciodată compromise**. Vulnerabilități noi sunt publicate zilnic, de aceea este recomandată o verificare periodică. Acest raport nu reprezintă o evaluare de conformitate, un audit sau o certificare în sensul RGPD, NIS2, ISO/IEC 27001, PCI DSS sau al oricărui alt cadru; referințele la aceste cadre sunt oferite doar pentru orientare.

DESPRE ACEST EXEMPLU

Companie fictivă, domenii rezervate pentru exemple (RFC 2606) și adrese IP de documentare (RFC 5737). Toate constatările și dovezile sunt ilustrative. Proiectele sunt contractate și facturate prin VAR24 INTERNATIONAL SRL.

Sergiu Vlad

Evaluare și remediere de securitate · me@sergiuvlad.com · sergiuvlad.com