Sergiu Vlad

SERGIUVLAD.COM

SECURITY ASSESSMENT REPORT

External exposure and web application assessment

Brightvale Freight SRL (fictional): public internet presence, mail server and the customer portal at app.example.com.

SAMPLE — FICTIONAL COMPANY, ILLUSTRATIVE FINDINGS

This sample shows the structure and depth of a real report. The company, domains (RFC 2606), IP addresses (RFC 5737), evidence and findings are invented for illustration.

CLIENT Brightvale Freight SRL (fictional)	ENGAGEMENT Vulnerability assessment
SCOPE External exposure snapshot + web application vulnerability assessment	PERIOD 2026 (testing and retest)
REPORT SV-SAMPLE-2026-01, version 1.1 (includes retest)	CLASSIFICATION Confidential — sample

PREPARED BY
Sergiu Vlad

me@sergiuvlad.com · sergiuvlad.com

01

Executive summary

What was tested, what was found, and what to do first, in plain business language.

Brightvale Freight asked for a vulnerability assessment of its public internet presence and of its customer portal, **app.example.com**. Testing ran in 2026 under a signed authorization, within an agreed window and without disrupting live systems.

I found **eight issues**. None is critical, but **two are high risk** and should be fixed within days: an outdated plugin on the public website that exposes customer enquiry data, and an administrator login that can be guessed without limit. Both could be used by an attacker with no inside knowledge.

Email sent in the name of example.com can currently be imitated, which makes fake-invoice fraud against customers easier. Three company accounts appear in public breach data. No signs of an active compromise were observed within the scope of this assessment.

After the retest, **six of eight findings are fixed and verified**. The remaining two have owners and dates. Overall exposure moved from **Elevated** to **Low**.

OVERALL EXPOSURE — INITIAL

Elevated

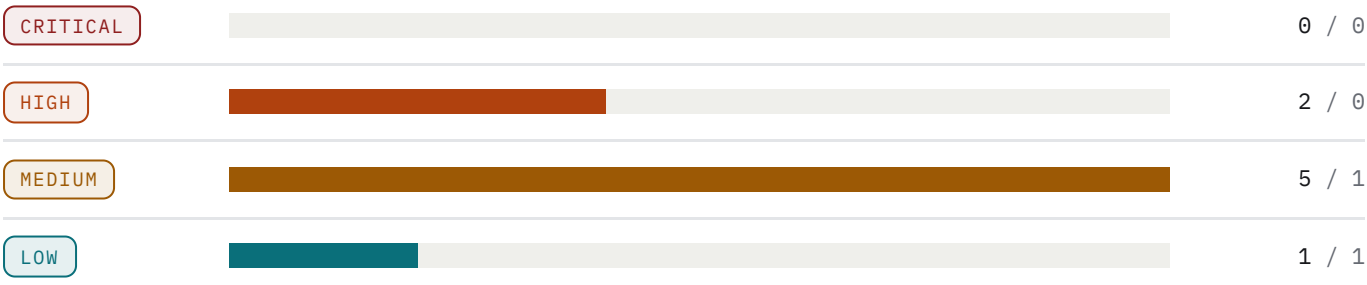
Two high-risk issues reachable from the internet without credentials.

OVERALL EXPOSURE — AFTER RETEST

Low

No high-risk issues remain. Two lower-risk items are scheduled.

RISK OVERVIEW (FINDINGS BY SEVERITY) — INITIAL / OPEN AFTER RETEST



Bars show the initial assessment. Grey figures: findings still open after the retest.

TOP THREE ACTIONS

01 **Update the website plugin** flagged in F-01 and remove plugins that are not used.

02 **Protect the admin login** with multi-factor authentication, rate limiting and an IP allow list.

03 **Finish email authentication**: sign all outgoing mail (DKIM) and enforce DMARC, so nobody can send invoices in your name.

02

Scope and methodology

Only the assets below were tested, under a written authorization. Anything not listed was out of scope.

ASSETS IN SCOPE

ASSET	DESCRIPTION	TESTING
`example.com`, `www.example.com`	Public website (content management system)	Passive snapshot, vulnerability assessment
`app.example.com`	Customer portal (web application and API)	Vulnerability assessment, authenticated with two test accounts (customer, dispatcher)
`mail.example.com`	Mail server (SMTP, IMAP)	Passive snapshot, TLS review
`staging.example.com`	Found during discovery; confirmed in scope by the client in writing	Vulnerability assessment
`203.0.113.0/28`	Public IP range, 16 addresses	External service review

Out of scope: internal network, staff (no phishing), denial-of-service, physical access, and third-party services beyond their DNS and email records.

HOW THE WORK WAS DONE

01	**Authorization**	Signed authorization and rules of engagement (ref. AUTH-SAMPLE-2026-01): assets, testing window, contacts, stop conditions.
02	**Passive discovery**	Public DNS, certificate transparency logs, search engines and public breach-data indexes. No traffic sent to client systems.
03	**Assessment**	AI-assisted scanning and analysis; every finding validated manually. OWASP WSTG for the website and portal. No destructive tests, no denial-of-service.
04	**Rating**	CVSS v3.1 base score, adjusted for business context. Mapped to MITRE ATT&CK where relevant.
05	**Report and retest**	Debrief with the client team, then a retest of each fix. This version (1.1) includes the retest results.

STANDARDS

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

03

Findings

Ordered by severity. Evidence is shortened and redacted; full evidence stays with the client team.

F-01

HIGH

Outdated website plugin with a publicly known vulnerability

CVSS V3.1 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N ASSET www.example.com

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

WHAT I FOUND

The contact-form plugin (name withheld in this sample) runs version 3.2.1. This version is affected by a known vulnerability listed in public advisories: unauthenticated SQL injection, fixed by the vendor in 3.2.4.

BUSINESS IMPACT

An attacker could read the website database, including customer enquiries (names, phone numbers, shipment details). That is a personal data breach under GDPR, with notification duties.

RETEST FIXED

Version 3.2.5 confirmed; the test request is no longer delayed. Two unused plugins removed.

EVIDENCE · ILLUSTRATIVE, REDACTED

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

POST /forms/submit (time-based test, 1 request)
-> response delayed 5.0 s; no data extracted
```

REMEDIATION

- Update the plugin to 3.2.4 or later; enable automatic security updates.
- Remove plugins that are installed but not used.
- Review web server logs for earlier exploitation attempts.

F-02

HIGH

Admin login exposed without multi-factor authentication or rate limiting

CVSS V3.1 7.4 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N ASSET www.example.com/admin/

REFERENCE WSTG-ATHN-03 · ATT&CK T1110

WHAT I FOUND

The website administration login is reachable from any IP address. It allows unlimited password attempts, shows no CAPTCHA or delay, and does not ask for a second factor.

BUSINESS IMPACT

A guessed or reused password gives full control of the public website: defacement, malicious downloads for visitors, or a fake payment page under your brand.

RETEST FIXED

MFA enforced for 4 admin accounts; /admin/ returns 403 outside the allow list.

EVIDENCE · ILLUSTRATIVE, REDACTED

```
POST /admin/login × 50 in 60 s (invalid password,
test account)
-> 50 × HTTP 200 "Invalid credentials"
-> no lockout, no delay, no MFA prompt
```

REMEDIATION

- Enable multi-factor authentication for every admin account.
- Add rate limiting and temporary lockout after failed attempts.
- Restrict /admin/ to the office IP or VPN.

F-03

MEDIUM

SSH open to the internet with password authentication

CVSS V3.1 6.5 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N ASSET 203.0.113.10:22 REFERENCE ATT&CK T1133 · T1110.001

WHAT I FOUND

The server at 203.0.113.10 accepts SSH logins with a password from any IP address. Automated password-guessing traffic against such servers is constant on the internet.

BUSINESS IMPACT

One weak or reused password would give an attacker a foothold on the server that hosts the staging site and nightly backups.

RETEST FIXED

Only publickey is offered; port 22 is filtered from outside the allow list.

EVIDENCE · ILLUSTRATIVE, REDACTED

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

REMEDIATION

- Allow key-based authentication only (PasswordAuthentication no).
- Limit port 22 to the VPN or known admin IPs.

F-04

MEDIUM

Outdated TLS versions and weak ciphers on the mail server

CVSS V3.1 Not scored (context) ASSET mail.example.com:443, :587, :993 REFERENCE WSTG-CRYP-01

WHAT I FOUND

The mail server still accepts TLS 1.0 and TLS 1.1 and offers legacy cipher suites (3DES, CBC with SHA-1). Current guidance is TLS 1.2 or later with modern ciphers.

BUSINESS IMPACT

Weakens the protection of email and passwords in transit, and fails the checks used by many client security questionnaires and insurers.

RETEST FIXED

Only TLS 1.2 and 1.3 offered; no legacy ciphers.

EVIDENCE · ILLUSTRATIVE, REDACTED

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

REMEDIATION

- Disable TLS 1.0 and 1.1; keep TLS 1.2 and 1.3.
- Use a modern cipher profile (forward secrecy, AEAD ciphers only).

F-05

MEDIUM

Directory listing on the staging subdomain

CVSS V3.1 5.3 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N ASSET staging.example.com/builds/ REFERENCE WSTG-CONF-04

WHAT I FOUND

The staging site is public and lists the contents of /builds/: old release archives and an example configuration file that reveals internal hostnames and the software stack.

BUSINESS IMPACT

Gives an attacker a map of internal systems and old code to study offline. Staging sites are often less patched than production.

RETEST FIXED

staging.example.com now requires sign-in; /builds/ returns 401.

EVIDENCE · ILLUSTRATIVE, REDACTED

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

REMEDIATION

- Disable directory listing on the web server.
- Put staging behind authentication or the VPN; remove old archives.

F-06

MEDIUM

Company accounts present in public breach data

CVSS V3.1 Not scored (context) ASSET @example.com accounts REFERENCE ATT&CK T1078

WHAT I FOUND

3 accounts on the example.com domain appear in 2 public breach datasets from third-party services. Only affected accounts and counts are reported; passwords were not collected or viewed.

BUSINESS IMPACT

If staff reused those passwords at work, an attacker could sign in to email or the portal as a legitimate user.

RETEST FIXED

Client confirmed the password resets; MFA prompt verified on the webmail sign-in for the 3 accounts.

EVIDENCE · ILLUSTRATIVE, REDACTED

```
a[redacted]@example.com   2 datasets
o[redacted]@example.com   1 dataset
s[redacted]@example.com   1 dataset
```

REMEDIATION

- Reset the passwords of the 3 accounts; enforce MFA on email.
- Turn on breach-password screening for new passwords.

F-07

MEDIUM

Email can be spoofed: DMARC not enforced, DKIM missing for one sender

CVSS V3.1 Not scored (context) ASSET example.com (DNS) REFERENCE Email authentication · ATT&CK T1566

WHAT I FOUND

The DMARC policy is p=none (monitor only), and the invoicing service that sends on behalf of example.com does not sign with DKIM. Receiving servers are not told to reject forged mail.

BUSINESS IMPACT

Fraudsters can send convincing fake invoices with changed bank details from your real domain to your customers.

RETEST IN PROGRESS

DKIM active for all senders; DMARC at p=quarantine. p=reject planned after 4 weeks of clean reports.

EVIDENCE · ILLUSTRATIVE, REDACTED

```
$ dig +short TXT _dmarc.example.com
"v=DMARC1; p=none; rua=mailto:dmarc@example.com"
$ dig +short TXT [redacted]._domainkey.example.com
(no record)
```

REMEDIATION

- Enable DKIM for every service that sends as example.com.
- Move DMARC to p=quarantine, then p=reject after reviewing reports.

F-08

LOW

Missing security headers on the customer portal

CVSS V3.1 Not scored (context) ASSET app.example.com
REFERENCE WSTG-CONF-07 · OWASP Secure Headers Project

WHAT I FOUND

Responses lack Content-Security-Policy, Strict-Transport-Security and a frame-ancestors rule. No exploitable issue was found, but these headers limit the damage of future bugs.

BUSINESS IMPACT

Defense in depth: without these headers, a future cross-site scripting flaw or clickjacking attempt has more room to succeed.

RETEST PLANNED

Scheduled for the next portal release; to be verified on request or in a quarterly check.

EVIDENCE · ILLUSTRATIVE, REDACTED

```
HTTP/2 200
content-type: text/html; charset=utf-8
(no content-security-policy)
(no strict-transport-security)
```

REMEDIATION

- Add HSTS and frame-ancestors 'none'.
- Introduce a Content-Security-Policy in report-only mode, then enforce it.

04

Remediation plan

Prioritized by risk and effort. Effort is an estimate for the client team; I can do the hands-on work if preferred, quoted separately.

FINDING	ACTION	EFFORT	OWNER
NOW — WITHIN 7 DAYS			
F-01	Update the plugin, remove unused plugins, check logs	1–2 hours	Web agency
F-02	MFA for admins, rate limiting, IP allow list	2–4 hours	Web agency
F-06	Reset 3 passwords, enforce MFA on email	1 hour	IT
NEXT — WITHIN 30 DAYS			
F-03	Key-only SSH, restrict port 22	1 hour	IT
F-04	Disable TLS 1.0/1.1 and legacy ciphers	1–2 hours	IT
F-05	Disable listing, put staging behind sign-in	1 hour	Web agency
F-07	DKIM for all senders, DMARC p=quarantine	2 hours	IT
LATER — WITHIN 90 DAYS			
F-07	DMARC p=reject after reviewing reports	30 min	IT
F-08	HSTS, frame-ancestors, CSP (report-only first)	0.5–1 day	Portal team
–	Recommended: quarterly external check to catch new exposure (Protect package)	Recurring	Client decision

05

Retest results

Each fix was checked again with the same method as the original finding. The report closes with proof, not promises.

6	1	1
FIXED AND VERIFIED	IN PROGRESS	PLANNED
F-01, F-02, F-03, F-04, F-05, F-06	F-07	F-08

Residual risk after retest: Low. No high-risk issue remains open. F-07 is partly fixed (DKIM active, DMARC at p=quarantine) and moves to p=reject after four weeks of clean reports; F-08 ships with the next portal release. Both can be verified on request or in a quarterly check.

06

Appendix

A. RATING METHOD

Severity follows the CVSS v3.1 base score: **Critical** 9.0–10.0, **High** 7.0–8.9, **Medium** 4.0–6.9, **Low** 0.1–3.9. The score is then read in business context (data involved, exposure, ease of exploitation).

Findings without a specific technical exploit path (accounts in breach data, email authentication, transport security and hardening headers) are rated on context, not with a CVSS vector, and marked "not scored": reachability from the internet and what an attacker gains decide the level.

B. AUTHORIZATION

All testing was performed under a written authorization signed by an authorized representative of the client (ref. AUTH-SAMPLE-2026-01), covering only the assets in section 02, within the agreed window. The client confirmed that it owns or controls each asset.

C. CONFIDENTIALITY

This report is confidential and intended for the client. Findings, evidence and any data encountered are handled under NDA and stored encrypted. Raw evidence is deleted 30 days after the final report; the report and the signed authorization are kept for 12 months as a record of the engagement, then deleted or returned, as the client prefers.

Passwords from breach data are never collected or reported: only affected accounts and counts.

D. LIMITATIONS

Results reflect the systems in scope during the testing window. An assessment reduces risk and documents due care; **it cannot guarantee that systems will never be breached**. New vulnerabilities are published every day, so a recurring check is recommended. This report is not a compliance assessment, audit or certification under GDPR, NIS2, ISO/IEC 27001, PCI DSS or any other framework; references to those frameworks are orientation only.

ABOUT THIS SAMPLE

Fictional company, reserved example domains (RFC 2606) and documentation IP addresses (RFC 5737). All findings and evidence are illustrative. Engagements are contracted and invoiced through VAR24 INTERNATIONAL SRL.

Sergiu Vlad

Security assessment and remediation · me@sergiuvlad.com · sergiuvlad.com