

CABINET DÉMO

Web application test

Security assessment report

PREPARED BY	Cabinet Démo
DATE	06/08/2026
SCOPE	Public web application

Executive dashboard

9	0	4
VULNERABILITIES	CRITICAL	HIGH
4	7.5	1
AFFECTED ASSETS	AVERAGE CVSS	REMOTE / UNAUTHENTICATED

[illegible]

Business impact

Concrete consequences for the business if the major exposures are left untreated.

F-001 Exposed .env file

Exposure of credentials or secrets could allow an attacker to access backend systems or third-party services, leading to data compromise.

NET-A-H1:443, NET-B-H1:443

F-002 Cross Site Scripting (Reflected)

An attacker could execute arbitrary JavaScript in the context of a victim's session, potentially leading to session hijacking or credential theft.

HOST-01:443

F-003 SQL Injection

An attacker could read, modify, or delete data in the underlying database, potentially compromising confidentiality and integrity of application data.

HOST-01:443

Remediation roadmap

Phase 1 IMMEDIATE · 0-7 DAYS 4 FINDINGS

Contain remote code execution and unauthenticated access.

Owner: Security engineering · Effort: Medium

F-001, F-002, F-003, F-004

Phase 2

Fix high-severity services and remove weak credentials.

Owner: Security engineering · Effort: Low

F-005, F-006

Phase 3 MEDIUM TERM · 31-90 DAYS 3 FINDINGS

Harden configuration, TLS and monitoring; retest the scope.

Owner: Security engineering · Effort: Low

F-007, F-008, F-009

Document control

VERSION	1.0
DATE	06/08/2026
AUTHOR	Cabinet Démo
CLASSIFICATION	Confidential — restricted distribution
DISTRIBUTION	Client and issuing firm; do not redistribute without written consent.
CONTACT	Not provided

Executive summary

This audit covered the organization's web application and related infrastructure. The assessment identified several high-severity issues, including exposed credential files and injection-type vulnerabilities that affect data handling in customer-facing systems. Two additional medium-severity weaknesses relate to browser-level protections and encryption strength. None of the identified issues are known to be actively exploited in the wild at this time. Management should prioritize remediation of the high-severity findings to reduce exposure of sensitive data and customer information.

Top risks

- Customer and order data could be accessed, altered, or deleted by an attacker exploiting weaknesses in the online shop's database handling.
- Exposed credentials could give an attacker a path into backend systems or connected third-party services, risking broader data compromise.
- Weaknesses in session and browser-level protections could allow an attacker to hijack user sessions or steal login credentials, undermining customer trust.

Severity distribution

SEVERITY	#	%	
CRITICAL	0	0%	
HIGH	4	44%	
MEDIUM	2	22%	
LOW	1	11%	
INFO	2	22%	

Scope and methodology

In scope

Public web application

4 host(s)

NET-A-H1, NET-B-H1, HOST-01, NET-B-H2

Out of scope

Any asset absent from the supplied exports. No active exploitation, no social engineering, no denial-of-service testing.

Files analysed

FILE	DETECTED TOOL	STATE
zap-sample.json	ZAP	Parsed
zap-sample.xml	ZAP	Parsed
burp-sample.xml	BURP	Parsed
nuclei-sample.jsonl	NUCLEI	Parsed

Methodology and limitations

Data comes from automated scanner exports (Nmap, Nessus, Trivy, Nuclei, Burp Suite, OWASP ZAP). Findings are correlated and deduplicated across tools, scored from CVSS and mapped to the relevant technical controls.

No external enrichment could be applied (CISA KEV and EPSS unavailable): ratings rest on CVSS and the severities reported by the tools alone.

Ce rapport est établi à partir de scans automatisés et ne constitue pas un test d'intrusion complet.

This report is based on automated scans and does not constitute a full penetration test.

Rating and prioritisation method

Severity scale

SEVERITY	CVSS
CRITIQUE / CRITICAL	9.0 - 10.0
ÉLEVÉE / HIGH	7.0 - 8.9
MOYENNE / MEDIUM	4.0 - 6.9
FAIBLE / LOW	0.1 - 3.9
INFO	0.0

Applied adjustments

Two adjustments may raise a finding by one level, capped at CRITICAL. Every applied adjustment is stated on the finding it affects:

- +1 level — public exposure observed (open port on a routable address).
- +1 level — known exploitation (present in the CISA KEV catalogue, or an exploit reported by the scanner).

No compliance percentage is calculated. The controls cited are evidence; the conformity decision belongs to the auditor.

Priority meanings

PRIORITY	
1	À traiter immédiatement / Immediate
2	À planifier dans le cycle courant / Planned
3	À suivre / Monitor

Findings summary

REF	TITLE	SEVERITY	CVSS	PRIORITY	STATUS
F-001	Exposed .env file	HIGH	7.5	1	Open
F-002	Cross Site Scripting (Reflected)	HIGH		1	Open
F-003	SQL Injection	HIGH		1	Open
F-004	SQL injection	HIGH		1	Open
F-005	Content Security Policy (CSP) Header Not Set	MEDIUM		2	Open
F-006	Weak TLS cipher	MEDIUM		2	Open
F-007	Nginx detected	INFO		3	Open
F-008	Timestamp Disclosure	INFO		3	Open
F-009	Low-severity observations — configuration	LOW		3	Open

Findings — detail

Extract: 3 of 9 findings are written up below. The remaining 6, their evidence and the remediation plan are in the full report.

F-001 Exposed .env file

HIGH CVSS 7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N CWE-200 Sources: NUCLEI

Sévérité high : score CVSS de 7.5.

CVSS detail — Attack vector: Network · Complexity: Low · Privileges required: None · User interaction: None · Scope: Unchanged · Confidentiality: High · Integrity: None · Availability: None

AFFECTED ASSETS

NET-A-H1:443, NET-B-H1:443

A .env file was found exposed on two internet-facing assets. This file type typically contains application configuration data such as credentials or API keys. The exposure was confirmed by an automated scan matching the exposed-env-file template.

IMPACT

Exposure of credentials or secrets could allow an attacker to access backend systems or third-party services, leading to data compromise.

EVIDENCE

```
Template: exposed-env-file
Matched at: https://NET-A-H1/.env

Template: exposed-env-file
Matched at: https://NET-B-H1/.env
Extracted: DB_PASSWORD=redacted
```

VERIFICATION

To verify, run: `nuclei -id exposed-env-file -u https://NET-A-H1`

REMEDIATION — PRIORITY 1 (IMMEDIATE)

Remove the .env file from the web-accessible directory immediately. Rotate any credentials or secrets that were present in the file. Configure the web server to block access to dotfiles. Verify no other configuration files are similarly exposed.

REFERENCES

<https://cwe.mitre.org/data/definitions/200.html>
<https://github.com/projectdiscovery/nuclei-templates/search?q=exposed-env-file>

Mapped controls: A.8.12, A.8.3, 21.2.i, 21.2.e · Status: Open

F-002 Cross Site Scripting (Reflected)

HIGH CWE-79 Sources: ZAP

Sévérité high : sévérité rapportée par l'outil (high).

AFFECTED ASSETS

HOST-01:443

A reflected Cross Site Scripting vulnerability was identified on the search functionality of the application. The 'q' parameter reflects unsanitized input, as demonstrated by the injected script tag being returned in the response.

IMPACT

An attacker could execute arbitrary JavaScript in the context of a victim's session, potentially leading to session hijacking or credential theft.

EVIDENCE

```
URI: https://HOST-01/search
Method: GET
Parameter: q
Evidence: <script>alert(1)</script>
```

REMEDIATION — PRIORITY 1 (IMMEDIATE)

Sanitize and encode all user-supplied input before rendering it in HTML output. Apply context-aware output encoding on the affected parameter. Implement a Content Security Policy as a defense-in-depth measure. Retest the endpoint after remediation.

REFERENCES

<https://cwe.mitre.org/data/definitions/79.html>

Mapped controls: A.8.26, A.8.28, 21.2.e · Status: Open

F-003 SQL Injection

HIGH CWE-89 Sources: ZAP

Sévérité high : sévérité rapportée par l'outil (high).

AFFECTED ASSETS

HOST-01:443

A SQL injection vulnerability was identified in the search functionality of the application. Injecting the payload ' OR '1'='1 into the 'q' parameter produced a SQL syntax error, indicating unsanitized input reaching the database layer.

IMPACT

An attacker could read, modify, or delete data in the underlying database, potentially compromising confidentiality and integrity of application data.

EVIDENCE

```
URI: https://HOST-01/search
Method: GET
Parameter: q
Attack: ' OR '1'='1
Evidence: SQL syntax error
```

REMEDIATION — PRIORITY 1 (IMMEDIATE)

Use parameterized queries or prepared statements for all database interactions. Remove any dynamic SQL construction from user input. Apply input validation as a secondary control. Retest the affected parameter after remediation.

REFERENCES

<https://cwe.mitre.org/data/definitions/89.html>

Mapped controls: A.8.26, A.8.28, 21.2.e · Status: Open

Remediation roadmap

Immediate (priority 1)

Ce plan de remédiation organise les actions selon trois horizons de priorité, sans échéance chiffrée imposée. Quatre findings de sévérité haute nécessitent une intervention sans délai : l'exposition d'un fichier .env (F-001), une vulnérabilité XSS réfléchie (F-002) et deux cas d'injection SQL (F-003, F-004). Aucun de ces findings n'est marqué KEV, mais leur sévérité haute justifie un traitement prioritaire. Ces failles touchent directement la confidentialité des données et l'intégrité applicative, ce qui impose une correction avant toute autre action.

F-001 — Exposed .env file

F-002 — Cross Site Scripting (Reflected)

F-003 — SQL Injection

F-004 — SQL injection

Planned (priority 2)

Deux findings de sévérité moyenne sont à intégrer au cycle de remédiation courant : l'absence d'en-tête Content Security Policy (F-005) et l'usage d'un chiffrement TLS faible (F-006). Ces éléments réduisent la robustesse défensive sans constituer une urgence immédiate. Leur correction doit être planifiée dans les travaux en cours, en cohérence avec les ressources disponibles.

F-005 — Content Security Policy (CSP) Header Not Set

F-006 — Weak TLS cipher

Monitor (priority 3)

Trois findings de sévérité faible ou informative sont à surveiller sans action immédiate : la détection du serveur Nginx (F-007), une divulgation d'horodatage (F-008), et des observations de configuration de faible sévérité (F-009). Ces éléments n'appellent pas de correction urgente mais doivent être réévalués lors du prochain audit.

F-007 — Nginx detected

F-008 — Timestamp Disclosure

F-009 — Low-severity observations — configuration

Annex — Control mapping

These are technical findings attached to the controls below as evidence. They are not a conformity assessment: no percentage is calculated and the conformity decision belongs to the auditor.

CONTRÔLE	INTITULÉ	FINDINGS
A.8.12	Data leakage prevention	F-001, F-008
A.8.24	Use of cryptography	F-006
A.8.26	Application security requirements	F-002, F-003, F-004, F-007
A.8.28	Secure coding	F-002, F-003, F-004, F-007
A.8.3	Information access restriction	F-001, F-008
A.8.9	Configuration management	F-005, F-009

NIS2

MESURE	INTITULÉ	FINDINGS
21.2.e	Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	F-001, F-002, F-003, F-004, F-007, F-008
21.2.f	Policies to assess the effectiveness of cybersecurity risk-management measures	F-005, F-009
21.2.g	Basic cyber hygiene practices and cybersecurity training	F-005, F-009
21.2.h	Policies on the use of cryptography and, where appropriate, encryption	F-006
21.2.i	Human resources security, access control policies and asset management	F-001, F-008
21.2.j	Use of multi-factor authentication, secured communications and secured emergency communication systems	F-006

Technical annex

REF	TITLE	SEVERITY	CVSS	ASSETS
F-001	Exposed .env file	HIGH	7.5	2
F-002	Cross Site Scripting (Reflected)	HIGH		1
F-003	SQL Injection	HIGH		1
F-004	SQL injection	HIGH		1
F-005	Content Security Policy (CSP) Header Not Set	MEDIUM		1
F-006	Weak TLS cipher	MEDIUM		1
F-007	Nginx detected	INFO		1
F-008	Timestamp Disclosure	INFO		1
F-009	Low-severity observations — configuration	LOW		1

Annex — Re-test

To be completed during remediation verification.

REF	TITLE	STATUS	DATE	VERIFICATION
F-001	Exposed .env file	Open		
F-002	Cross Site Scripting (Reflected)	Open		
F-003	SQL Injection	Open		
F-004	SQL injection	Open		
F-005	Content Security Policy (CSP) Header Not Set	Open		
F-006	Weak TLS cipher	Open		
F-007	Nginx detected	Open		
F-008	Timestamp Disclosure	Open		
F-009	Low-severity observations — configuration	Open		