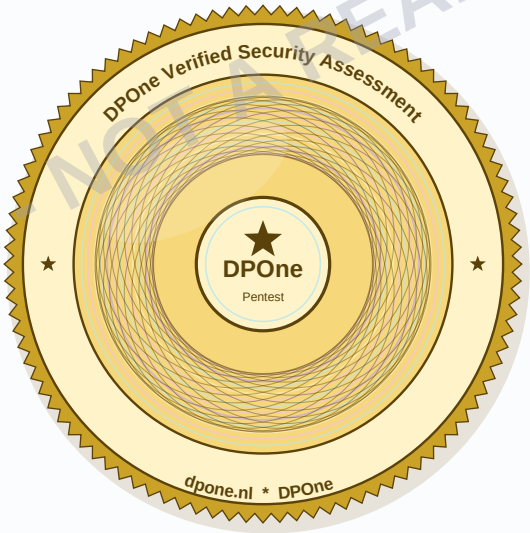
STRICTLY CONFIDENTIAL

Penetration Test Report

Automated non-destructive security assessment

example.com

SAMPLE - NOT A REAL ASSESSMENT



Customer	**Example B.V. (SAMPLE)**
Target	**example.com**
Testing period	**2 November 2026 - 2 November 2026**
Issued	**2 November 2026**
Report ID	**ptsample00000000000**
Add-ons	**-**

SAMPLE - NOT A REAL ASSESSMENT

Strictly confidential - contains unremediated security weaknesses.

Customer's authorised contacts only. Do not forward without the customer's consent.

MBZ Compliance · Vegelinsoord 148, 3079KN Rotterdam · KvK 98446932 · BTW NL005331884B84 · dpone.nl

Document control

Report ID	ptsample00000000000
Version	1.0 - final
Prepared for	Example B.V. (SAMPLE) - example.com
Prepared by	DPOne - MBZ Compliance, Rotterdam, the Netherlands (KvK 98446932)
Issued	2 November 2026
Classification	Strictly confidential - contains unremediated security weaknesses.
Distribution	Customer's authorised contacts only. Do not forward without the customer's consent.
Results fingerprint (SHA-256)	SAMPLE-NOT-A-REAL-FINGERPRINT
Engine	DPOne automated engine pentest-1.0.0

Contents

1. Executive summary 3
2. Scope and authorisation 4
3. Methodology 5
4. Findings summary 6
5. Detailed findings 7
6. Remediation roadmap 11
7. Checklist coverage matrix 12
8. Appendix A - References 14
9. Appendix B - Glossary in plain language 15
10. Disclaimer 15
11. Sign-off 16

SAMPLE - NOT A REAL ASSESSMENT

Executive summary

DPOne carried out an automated, non-destructive security assessment of example.com for Example B.V. (SAMPLE). 15 checks were executed across the agreed scope. 6 finding(s) need attention; the overall security score is 70/100.

Overall risk
Medium

Security score
70/100

Findings by severity



Most important findings

- F-01 [Medium] No Content-Security-Policy header
- F-02 [Medium] Vulnerable library: jQuery 3.4.1
- F-03 [Medium] HSTS header missing

Strengths observed

- Cookies are Secure and HttpOnly
- CORS does not reflect arbitrary origins
- DNSSEC enabled
- HTTP redirects to HTTPS
- HTTPS available with a valid certificate
- No exposed .git repository

SAMPLE - NOT A REAL ASSESSMENT

Scope and authorisation

The assessment covered the verified target listed below and, where purchased, the uploaded application builds.

In scope

- example.com (DNS, HTTPS, web application surface)

Out of scope

Third-party services and domains, authenticated application areas, denial-of-service, social engineering, physical security and any system not listed in scope.

Written authorisation

Testing was authorised in writing by Jane Example (CTO, Example B.V.) on 1 November 2026, for the window 2 November 2026 to 9 November 2026. Domain ownership was verified before any test traffic was sent.

Rules of Engagement

- Non-destructive tests only; no data was modified or deleted.
- No denial-of-service, load testing, brute force or social engineering.
- No exploitation beyond safe proof (harmless markers only).
- Rate-limited requests with an identifiable user agent.
- Uploaded apps were analysed statically and never executed.

Applications analysed

No application builds were in scope.

SAMPLE - NOT A REAL ASSESSMENT

Methodology

The assessment follows the phases of PTES and NIST SP 800-115 (planning, discovery, assessment, reporting) and uses the OWASP Web Security Testing Guide (WSTG v4.2) test cases that can be performed safely and automatically from the internet.

Results are mapped to OWASP ASVS 4.0.3 requirements, the OWASP Top 10:2021, CWE and, for mobile apps, OWASP MASVS v2 / MASTG. Known vulnerabilities are matched against NVD, CISA KEV, OSV, GitHub Security Advisories and retire.js data that DPOne refreshes daily.

The test plan follows DPOne's 21-section penetration-test checklist (458 items). The coverage matrix shows which sections were tested automatically and which require manual review.

Standards

- OWASP WSTG v4.2
- OWASP ASVS 4.0.3 / 5.0
- OWASP Top 10:2021
- OWASP MASVS v2 / MASTG
- PTES
- NIST SP 800-115
- CVSS v3.1 (FIRST)
- CWE (MITRE)
- DPOne penetration-test checklist (21 sections, 458 items)

Severity and scoring

Severity is DPOne's contextual rating for this target. The CVSS v3.1 base score shows the generic severity of the weakness class (vector included for transparency). The security score starts at 100 and subtracts 25/15/7/3 points per critical/high/medium/low finding.

Severity	Impact
Critical	Can lead to full compromise of the asset or its data with little effort.
High	Can lead to serious data exposure or account/system compromise.
Medium	Weakens defences and can be combined with other issues to cause harm.
Low	Minor weakness or missing hardening; low direct risk.
Info	Informational observation; no direct risk.

SAMPLE - NOT A REAL ASSESSMENT

Findings summary

ID	Finding	Severity	Asset	CVSS	Priority
F-01	No Content-Security-Policy header	Medium	example.com	4.7	P2
F-02	Vulnerable library: jQuery 3.4.1	Medium	example.com	4.7	P2
F-03	HSTS header missing	Medium	example.com	3.7	P2
F-04	Clickjacking protection missing	Low	example.com	4.3	P3
F-05	DMARC policy is p=none	Low	example.com	4.3	P3
F-06	No security.txt published	Low	example.com	-	P3

SAMPLE - NOT A REAL ASSESSMENT

Detailed findings

F-01 No Content-Security-Policy header

Severity	Medium (P2)
CVSS v3.1	4.7 - CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N
Affected asset	example.com
Category	Security headers
Checklist section	5.1

Evidence (sanitised)

GET https://example.com/ returned 200 without a Content-Security-Policy header.

Impact

Weakens defences and can be combined with other issues to cause harm.

Remediation

1. Define a Content-Security-Policy that allows only your own origins.
2. Start in Report-Only mode, review violations, then enforce it.
3. Avoid 'unsafe-inline' by using nonces.
4. Retest with DPOne to confirm the fix.

References

OWASP WSTG WSTG-CONF-12 - https://owasp.org/www-project-web-security-testing-guide/v42/
OWASP ASVS 4.0.3 V14.4.3 - https://github.com/OWASP/ASVS/tree/v4.0.3
OWASP Top 10 A05:2021 Security Misconfiguration - https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
CWE-693 - https://cwe.mitre.org/data/definitions/693.html

Retest status Open - free automated retest available for 30 days

F-02 Vulnerable library: jQuery 3.4.1

Severity	Medium (P2)
CVSS v3.1	4.7 - CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N
Affected asset	example.com
Category	Third-party JavaScript
Checklist section	15.2

Evidence (sanitised)

https://example.com/js/jquery-3.4.1.min.js matches jQuery 3.4.1 (retire.js). Known advisories: CVE-2020-11022, CVE-2020-11023.

Impact

Weakens defences and can be combined with other issues to cause harm.

Remediation

1. Upgrade jQuery to 3.7.1 or later.
2. Remove unused copies of the library.
3. Add Subresource Integrity for third-party scripts.
4. Retest with DPOne to confirm the fix.

References

OWASP WSTG WSTG-INFO-08 - https://owasp.org/www-project-web-security-testing-guide/v42/
OWASP ASVS 4.0.3 V14.2.1 - https://github.com/OWASP/ASVS/tree/v4.0.3
OWASP Top 10 A06:2021 Vulnerable and Outdated Components - https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
CWE-1395 - https://cwe.mitre.org/data/definitions/1395.html
CVE-2020-11022 - https://nvd.nist.gov/vuln/detail/CVE-2020-11022
CVE-2020-11023 - https://nvd.nist.gov/vuln/detail/CVE-2020-11023

SAMPLE - NOT A REAL ASSESSMENT

Retest status Open - free automated retest available for 30 days

F-03 HSTS header missing

Severity Medium (P2)
CVSS v3.1 3.7 - CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N
Affected asset example.com
Category TLS
Checklist section 1.2

Evidence (sanitised)

Strict-Transport-Security header not present on https://example.com/.

Impact

Weakens defences and can be combined with other issues to cause harm.

Remediation

1. Send Strict-Transport-Security: max-age=31536000; includeSubDomains.
2. After verifying all subdomains use HTTPS, add preload and submit to hstspreload.org.
3. Retest with DPOne to confirm the fix.

References

OWASP WSTG WSTG-CONF-07 - https://owasp.org/www-project-web-security-testing-guide/v42/
OWASP ASVS 4.0.3 V14.4.5 - https://github.com/OWASP/ASVS/tree/v4.0.3
OWASP Top 10 A05:2021 Security Misconfiguration - https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
CWE-319 - https://cwe.mitre.org/data/definitions/319.html
hstspreload.org - https://hstspreload.org/

Retest status Open - free automated retest available for 30 days

F-04 Clickjacking protection missing

Severity Low (P3)
CVSS v3.1 4.3 - CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
Affected asset example.com
Category Security headers
Checklist section 5.1

Evidence (sanitised)

Neither X-Frame-Options nor CSP frame-ancestors is set.

Impact

Minor weakness or missing hardening; low direct risk.

Remediation

1. Add Content-Security-Policy: frame-ancestors 'self' (or X-Frame-Options: DENY for older browsers).
2. Retest with DPOne to confirm the fix.

References

OWASP WSTG WSTG-CLNT-09 - https://owasp.org/www-project-web-security-testing-guide/v42/
OWASP ASVS 4.0.3 V14.4.7 - https://github.com/OWASP/ASVS/tree/v4.0.3
OWASP Top 10 A05:2021 Security Misconfiguration - https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
CWE-1021 - https://cwe.mitre.org/data/definitions/1021.html

Retest status Open - free automated retest available for 30 days

SAMPLE - NOT A REAL ASSESSMENT

F-05 DMARC policy is p=none

Severity Low (P3)
CVSS v3.1 4.3 - CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
Affected asset example.com
Category Email security
Checklist section 1.1

Evidence (sanitised)

```
_dmarc.example.com TXT "v=DMARC1; p=none"
```

Impact

Minor weakness or missing hardening; low direct risk.

Remediation

1. Monitor DMARC aggregate reports for two to four weeks.
2. Move to p=quarantine and then to p=reject once all legitimate senders pass SPF or DKIM.
3. Retest with DPOne to confirm the fix.

References

OWASP Top 10 A05:2021 Security Misconfiguration - https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
CWE-290 - https://cwe.mitre.org/data/definitions/290.html
RFC 7489 (DMARC) - https://www.rfc-editor.org/rfc/rfc7489

Retest status Open - free automated retest available for 30 days

F-06 No security.txt published

Severity Low (P3)
Affected asset example.com
Category Disclosure
Checklist section 19

Evidence (sanitised)

```
GET /.well-known/security.txt returned 404.
```

Impact

Minor weakness or missing hardening; low direct risk.

Remediation

1. Publish /.well-known/security.txt with a Contact and an Expires field as defined in RFC 9116.
2. Retest with DPOne to confirm the fix.

References

OWASP Top 10 A05:2021 Security Misconfiguration - https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
RFC 9116 (security.txt) - https://www.rfc-editor.org/rfc/rfc9116

Retest status Open - free automated retest available for 30 days

SAMPLE - NOT A REAL ASSESSMENT

Observations (informational)

ID	Finding	Evidence (sanitised)
O-01	robots.txt reviewed	robots.txt lists /admin/ (path exists, login required).

Controls verified

The following checks passed:

Finding	Asset
Cookies are Secure and HttpOnly	example.com
CORS does not reflect arbitrary origins	example.com
DNSSEC enabled	example.com
HTTP redirects to HTTPS	example.com
HTTPS available with a valid certificate	example.com
No exposed .git repository	example.com
No open redirect on common parameters	example.com
No unencoded reflection of a harmless marker	example.com

SAMPLE - NOT A REAL ASSESSMENT

Remediation roadmap

Priority			ID
P1	Within 7 days	Critical and high findings	-
P2	Within 30 days	Medium findings	F-01, F-02, F-03
P3	Within 90 days	Low findings and hardening	F-04, F-05, F-06
P4	Planned	Observations and manual review items	1 observations + manual review items (see coverage)

P2 - Within 30 days

- F-01 No Content-Security-Policy header: Define a Content-Security-Policy that allows only your own origins.
- F-02 Vulnerable library: jQuery 3.4.1: Upgrade jQuery to 3.7.1 or later.
- F-03 HSTS header missing: Send Strict-Transport-Security: max-age=31536000; includeSubDomains.

P3 - Within 90 days

- F-04 Clickjacking protection missing: Add Content-Security-Policy: frame-ancestors 'self' (or X-Frame-Options: DENY for older browsers).
- F-05 DMARC policy is p=none: Monitor DMARC aggregate reports for two to four weeks.
- F-06 No security.txt published: Publish /.well-known/security.txt with a Contact and an Expires field as defined in RFC 9116.

SAMPLE - NOT A REAL ASSESSMENT

Checklist coverage matrix

Automated checks cover the parts of each section that can be tested safely from outside without credentials. Items not covered are marked for manual review.

Section	Items	Checks	Passed	Failed	Status
0. Governance, threat model and authorisation	21	0	0	0	Partly tested
1. Infrastructure, network, DNS and TLS	46	5	3	2	Partly tested
2. Backend and API	42	0	0	0	Not tested - manual review
3. Authentication and session management	29	1	1	0	Partly tested
4. Authorisation and access control	10	0	0	0	Not tested - manual review
5. Front-end and public website	38	6	3	2	Partly tested
6. Dashboards (customer and admin)	13	0	0	0	Not tested - manual review
7. Data, cryptography and secrets	18	0	0	0	Not tested - manual review
8. File upload and reports	10	0	0	0	Not tested - manual review
9. AI / LLM (OWASP LLM Top 10 2025)	30	0	0	0	Not tested - manual review
10. Mobile application (OWASP MASVS)	34	0	0	0	Out of scope
11. Windows desktop application	27	0	0	0	Out of scope
12. Telegram bot and mini app	24	0	0	0	Not tested - manual review
13. Cross-component trust	23	1	1	0	Partly tested
14. Payments and billing	6	0	0	0	Not tested - manual review
15. Supply chain, CI/CD and code	25	1	0	1	Partly tested
16. Logging, monitoring and detection	10	0	0	0	Not tested - manual review
17. Backup, continuity and incident response	11	0	0	0	Not tested - manual review
18. Privacy and legal compliance	11	0	0	0	Not tested - manual review
19. Security testing and vulnerability disclosure	13	1	0	1	Partly tested
20. Go-live checklist	17	0	0	0	Not tested - manual review

Not tested / requires manual review

The following areas were not tested automatically. DPOne can arrange a manual review on request (info@dpone.info).

- 0. Governance, threat model and authorisation: Architecture/data-flow diagram, STRIDE threat model, asset classification, policies, insurance.
- 1. Infrastructure, network, DNS and TLS: Firewall and open ports, origin IP exposure, TLS protocol/cipher enumeration, servers, containers, cloud IAM, registrar lock and 2FA.
- 2. Backend and API: Authenticated API testing: injection (SQL/NoSQL/command), SSRF, IDOR/BOLA, mass assignment, business logic, GraphQL/WebSocket, race conditions.
- 3. Authentication and session management: Password policy, MFA, password reset, JWT/refresh tokens, OAuth state/PKCE, session fixation (need test accounts).
- 4. Authorisation and access control: Horizontal/vertical privilege escalation and tenant isolation (needs two test accounts and roles).
- 5. Front-end and public website: DOM XSS, postMessage, CSRF on authenticated forms, client-side storage of tokens, CAPTCHA bypass.
- 6. Dashboards (customer and admin): Encoding of findings, signed downloads, CSV injection, audit log, impersonation, four-eyes approval.
- 7. Data, cryptography and secrets: Encryption at rest, key management/KMS, database hardening, Git history secret scanning.
- 8. File upload and reports: Upload validation, malware scanning, SVG/ZIP handling, HTML-to-PDF SSRF (needs authenticated

SAMPLE - NOT A REAL ASSESSMENT

testing).

- 9. AI / LLM (OWASP LLM Top 10 2025): Full red-teaming (jailbreaks), RAG tenant isolation, excessive agency, output handling, cost limits.
- 12. Telegram bot and mini app: Webhook secret, initData validation, command authorisation, callback_data IDOR (needs bot access).
- 13. Cross-component trust: Token audiences per channel, service-to-service auth, webhook signatures, integration test matrix.
- 14. Payments and billing: Server-side price calculation, webhook-only activation, idempotency, invoice IDOR (needs test checkout).
- 15. Supply chain, CI/CD and code: Repository protection, SAST, secret scanning, SBOM, CI secrets and runners.
- 16. Logging, monitoring and detection: Security event logging, SIEM, alerting (needs internal access).
- 17. Backup, continuity and incident response: 3-2-1 backups, restore tests, incident response plan and runbooks (document review).
- 18. Privacy and legal compliance: GDPR documentation, DPA, DPIA, NIS2/AI Act/CRA scoping (covered by DPOne's GDPR services).
- 19. Security testing and vulnerability disclosure: Independent manual pentest, bug bounty, red teaming, staff security.
- 20. Go-live checklist: Port scan, MFA on admin accounts, IDOR tests, backups, incident plan, third-party pentest.

SAMPLE - NOT A REAL ASSESSMENT

Appendix A - References

- OWASP Web Security Testing Guide (WSTG) v4.2 - https://owasp.org/www-project-web-security-testing-guide/v42/
- OWASP Application Security Verification Standard (ASVS) 4.0.3 - https://github.com/OWASP/ASVS/tree/v4.0.3
- OWASP ASVS 5.0 - https://github.com/OWASP/ASVS
- OWASP Top 10:2021 - https://owasp.org/Top10/
- OWASP Top 10 for LLM Applications 2025 - https://genai.owasp.org/llm-top-10/
- OWASP MASVS v2 and MASTG - https://mas.owasp.org/
- PTES - Penetration Testing Execution Standard - http://www.pentest-standard.org/
- NIST SP 800-115, Technical Guide to Information Security Testing and Assessment - https://csrc.nist.gov/pubs/sp/800/115/final
- FIRST CVSS v3.1 Specification - https://www.first.org/cvss/v3.1/specification-document
- MITRE CWE - https://cwe.mitre.org/
- NIST National Vulnerability Database - https://nvd.nist.gov/
- CISA Known Exploited Vulnerabilities Catalog - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- OSV.dev open source vulnerability database - https://osv.dev/
- RFC 9116 security.txt - https://www.rfc-editor.org/rfc/rfc9116
- Wetboek van Strafrecht art. 138ab (computervredebreuk) - https://wetten.overheid.nl/jci1.3:c:BWBR0001854&boek=Tweede&titeldeel=V&artikel=138ab

CVE / advisories

- CVE-2020-11022 - https://nvd.nist.gov/vuln/detail/CVE-2020-11022
- CVE-2020-11023 - https://nvd.nist.gov/vuln/detail/CVE-2020-11023

SAMPLE - NOT A REAL ASSESSMENT

Appendix B - Glossary in plain language

Penetration test
A controlled check of your systems by someone you asked, looking for weak spots before attackers do.

Finding
A weakness we found, with proof and a fix.

Severity
How bad a weakness is: critical, high, medium, low or informational.

CVSS
An international scoring system (0 to 10) for how serious a type of weakness is.

CVE
A public ID number for a known security bug in a product, like CVE-2024-1234.

CWE
A catalogue name for a type of mistake, like 'cross-site scripting' (CWE-79).

HTTPS / TLS
The padlock: it encrypts traffic between visitors and your site.

HSTS
A rule that tells browsers to always use the padlock version of your site.

Security headers
Small instructions your site sends to browsers to block common attacks.

SPF, DKIM, DMARC
Email settings that stop criminals sending mail that pretends to come from you.

DNSSEC
A digital seal on your domain's address book so nobody can redirect visitors.

XSS
A trick where an attacker gets their script to run inside your page.

Open redirect
A link on your site that can send people to any other site, useful for phishing.

Static analysis
Reading an app's files without running it.

Remediation
The fix.

Disclaimer

This report is a point-in-time assessment. It reflects the state of the target on the testing dates only.

It is limited to the agreed scope and to automated, non-destructive checks, unless stated otherwise. Absence of a finding does not prove absence of vulnerabilities. Areas marked 'not tested' were not assessed.

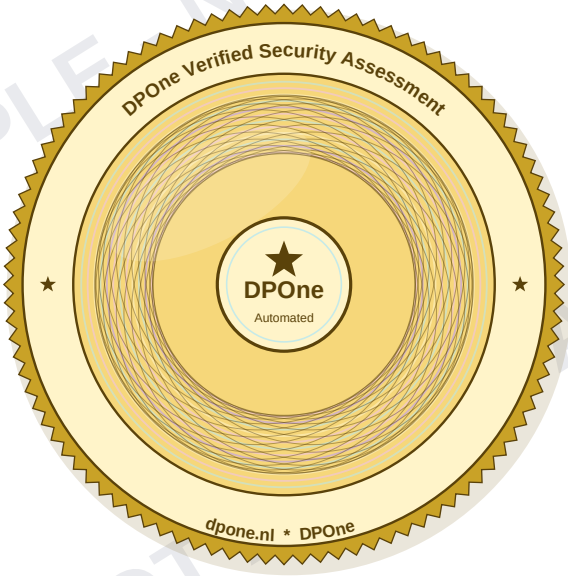
No human penetration tester performed manual exploitation for this report unless explicitly stated. The report does not constitute a certification or legal advice.

SAMPLE - NOT A REAL ASSESSMENT

Sign-off

This report was produced by DPOne's automated assessment engine under the authorisation described above and issued by DPOne (MBZ Compliance).

Issued by	DPOne - MBZ Compliance, Rotterdam, the Netherlands (KvK 98446932)
Report ID	ptsample00000000000
Issued	2 November 2026
Target	example.com
Results fingerprint (SHA-256)	SAMPLE-NOT-A-REAL-FINGERPRINT



DPOne Verified Security Assessment

Automated · Non-destructive · Authorised

Verify the authenticity of this report:
https://dpone.nl/verify/ptsample00000000000

SAMPLE - NOT A REAL ASSESSMENT