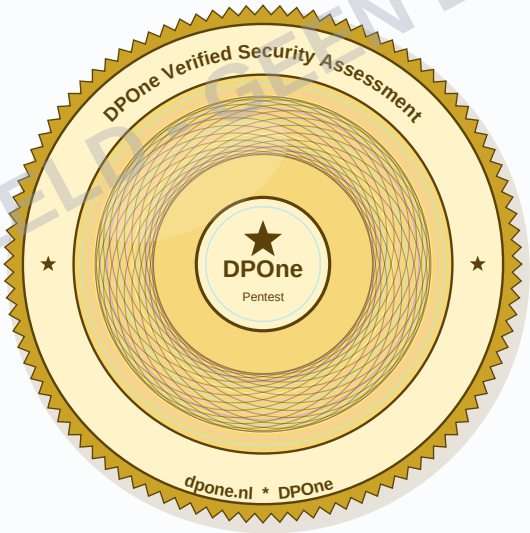
STRIKT VERTROUWELIJK

Penetratietestrapport

Geautomatiseerde, niet-destructieve beveiligingsbeoordeling

example.com

VOORBEELD - GEEN ECHTE BEOORDELING



Klant	**Example B.V. (SAMPLE)**
Doel	**example.com**
Testperiode	**2 november 2026 - 2 november 2026**
Uitgegeven	**2 november 2026**
Rapport-ID	**ptsample00000000000**
Add-ons	**-**

VOORBEELD - GEEN ECHTE BEOORDELING

Documentbeheer

Rapport-ID	ptsample00000000000
Versie	1.0 - definitief
Opgesteld voor	Example B.V. (SAMPLE) - example.com
Opgesteld door	DPOne - MBZ Compliance, Rotterdam, Nederland (KvK 98446932)
Uitgegeven	2 november 2026
Classificatie	Strikt vertrouwelijk - bevat niet-opgeloste beveiligingszwakheden.
Verspreiding	Alleen geautoriseerde contactpersonen van de klant. Niet doorsturen zonder toestemming van de klant.
Vingerafdruk resultaten (SHA-256)	SAMPLE-NOT-A-REAL-FINGERPRINT
Engine	DPOne automated engine pentest-1.0.0

Technische details van bevindingen (titels, bewijs en oplossingen) zijn in het Engels, zodat ze één-op-één aansluiten bij de internationale standaarden.

Inhoud

1. Managementsamenvatting 3
2. Scope en autorisatie 4
3. Methodologie 5
4. Overzicht bevindingen 6
5. Gedetailleerde bevindingen 7
6. Herstelplan 11
7. Dekkingsmatrix checklist 12
8. Bijlage A - Referenties 14
9. Bijlage B - Begrippenlijst in gewone taal 15
10. Disclaimer 15
11. Ondertekening 16

VOORBEELD - GEEN ECHTE BEOORDELING

Managementsamenvatting

DPOne heeft een geautomatiseerde, niet-destructieve beveiligingsbeoordeling uitgevoerd van example.com voor Example B.V. (SAMPLE). Er zijn 15 controles uitgevoerd binnen de afgesproken scope. 6 bevinding(en) vragen aandacht; de totale beveiligingsscore is 70/100.

Totaal risico
Gemiddeld

Beveiligingsscore
70/100

Bevindingen per ernst



Belangrijkste bevindingen

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

Sterke punten

- 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

VOORBEELD - GEEN ECHTE BEOORDELING

Scope en autorisatie

De beoordeling omvatte het hieronder vermelde geverifieerde doel en, indien afgenomen, de geüploade app-builds.

Binnen scope

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

Buiten scope

Diensten en domeinen van derden, afgeschermde delen van de applicatie, denial-of-service, social engineering, fysieke beveiliging en systemen die niet in de scope staan.

Schriftelijke autorisatie

Het testen is schriftelijk geautoriseerd door Jane Example (CTO, Example B.V.) op 1 november 2026, voor het venster 2 november 2026 tot 9 november 2026. Domeineigendom is geverifieerd voordat er testverkeer werd verstuurd.

Rules of Engagement

- Alleen niet-destructieve tests; er zijn geen gegevens gewijzigd of verwijderd.
- Geen denial-of-service, belastingtests, brute force of social engineering.
- Geen exploitatie verder dan veilig bewijs (alleen onschuldige markers).
- Begrensd aantal verzoeken met een herkenbare user agent.
- Geüploade apps zijn statisch geanalyseerd en nooit uitgevoerd.

Geanalyseerde applicaties

Er vielen geen app-builds binnen de scope.

VOORBEELD - GEEN ECHTE BEOORDELING

Methodologie

De beoordeling volgt de fasen van PTES en NIST SP 800-115 (planning, ontdekking, beoordeling, rapportage) en gebruikt de testgevallen uit de OWASP Web Security Testing Guide (WSTG v4.2) die veilig en geautomatiseerd vanaf internet kunnen worden uitgevoerd.

Resultaten zijn gekoppeld aan OWASP ASVS 4.0.3, de OWASP Top 10:2021, CWE en voor mobiele apps OWASP MASVS v2 / MASTG. Bekende kwetsbaarheden worden vergeleken met NVD, CISA KEV, OSV, GitHub Security Advisories en retire.js-data die DPOne dagelijks bijwerkt.

Het testplan volgt DPOne's penetratietest-checklist met 21 secties (458 punten). De dekkingsmatrix laat zien welke secties automatisch zijn getest en welke handmatige beoordeling vereisen.

Standaarden

- 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)

Ernst en score

De ernst is DPOne's contextuele beoordeling voor dit doel. De CVSS v3.1-basisscore toont de algemene ernst van het type zwakheid (vector ter transparantie). De score start op 100 en trekt 25/15/7/3 punten af per kritieke/hoge/gemiddelde/lage bevinding.

Ernst	Impact
Kritiek	Kan met weinig moeite leiden tot volledige compromittering van het asset of de data.
Hoog	Kan leiden tot ernstige datalekken of overname van accounts of systemen.
Gemiddeld	Verzwakt de verdediging en kan samen met andere problemen schade veroorzaken.
Laag	Kleine zwakheid of ontbrekende hardening; laag direct risico.
Info	Informatieve observatie; geen direct risico.

VOORBEELD - GEEN ECHTE BEOORDELING

Overzicht bevindingen

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

VOORBEELD - GEEN ECHTE BEOORDELING

Gedetailleerde bevindingen

F-01 No Content-Security-Policy header

Ernst	Gemiddeld (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
Getroffen asset	example.com
Categorie	Security headers
Checklistsectie	5.1

Bewijs (geschoond)

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

Impact

Verzwakt de verdediging en kan samen met andere problemen schade veroorzaken.

Oplossing

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.

Referenties

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

Hertest-status Open - free automated retest available for 30 days

F-02 Vulnerable library: jQuery 3.4.1

Ernst	Gemiddeld (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
Getroffen asset	example.com
Categorie	Third-party JavaScript
Checklistsectie	15.2

Bewijs (geschoond)

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

Verzwakt de verdediging en kan samen met andere problemen schade veroorzaken.

Oplossing

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.

Referenties

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

VOORBEELD - GEEN ECHTE BEOORDELING

Hertest-status Open - free automated retest available for 30 days

F-03 HSTS header missing

Ernst Gemiddeld (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
Getroffen asset example.com
Categorie TLS
Checklistsectie 1.2

Bewijs (geschoond)

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

Impact

Verzwakt de verdediging en kan samen met andere problemen schade veroorzaken.

Oplossing

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.

Referenties

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/

Hertest-status Open - free automated retest available for 30 days

F-04 Clickjacking protection missing

Ernst Laag (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
Getroffen asset example.com
Categorie Security headers
Checklistsectie 5.1

Bewijs (geschoond)

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

Impact

Kleine zwakheid of ontbrekende hardening; laag direct risico.

Oplossing

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

Referenties

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

Hertest-status Open - free automated retest available for 30 days

VOORBEELD - GEEN ECHTE BEOORDELING

F-05 DMARC policy is p=none

Ernst	Laag (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
Getroffen asset	example.com
Categorie	Email security
Checklistsectie	1.1

Bewijs (geschoond)

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

Impact

Kleine zwakheid of ontbrekende hardening; laag direct risico.

Oplossing

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.

Referenties

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

Hertest-status Open - free automated retest available for 30 days

F-06 No security.txt published

Ernst	Laag (P3)
Getroffen asset	example.com
Categorie	Disclosure
Checklistsectie	19

Bewijs (geschoond)

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

Impact

Kleine zwakheid of ontbrekende hardening; laag direct risico.

Oplossing

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.

Referenties

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

Hertest-status Open - free automated retest available for 30 days

VOORBEELD - GEEN ECHTE BEOORDELING

Observaties (informatief)

ID	Bevinding	Bewijs (geschoond)
O-01	robots.txt reviewed	robots.txt lists /admin/ (path exists, login required).

Geverifieerde maatregelen

De volgende controles zijn geslaagd:

Bevinding	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

VOORBEELD - GEEN ECHTE BEOORDELING

Herstelplan

Prioriteit			ID
P1	Binnen 7 dagen	Kritieke en hoge bevindingen	-
P2	Binnen 30 dagen	Gemiddelde bevindingen	F-01, F-02, F-03
P3	Binnen 90 dagen	Lage bevindingen en hardening	F-04, F-05, F-06
P4	Gepland	Observaties en handmatige controles	1 observations + manual review items (see coverage)

P2 - Binnen 30 dagen

- 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 - Binnen 90 dagen

- 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.

VOORBEELD - GEEN ECHTE BEOORDELING

Dekkingsmatrix checklist

Geautomatiseerde controles dekken de delen van elke sectie die veilig van buitenaf en zonder inloggegevens te testen zijn. Niet-gedekte punten zijn gemarkeerd voor handmatige beoordeling.

Sectie	Punten	Controles	Geslaagd	Gefaald	Status
0. Governance, dreigingsmodel en autorisatie	21	0	0	0	Deels getest
1. Infrastructuur, netwerk, DNS en TLS	46	5	3	2	Deels getest
2. Backend en API	42	0	0	0	Niet getest - handmatig
3. Authenticatie en sessiebeheer	29	1	1	0	Deels getest
4. Autorisatie en toegangscontrole	10	0	0	0	Niet getest - handmatig
5. Front-end en publieke website	38	6	3	2	Deels getest
6. Dashboards (klant en beheer)	13	0	0	0	Niet getest - handmatig
7. Data, cryptografie en secrets	18	0	0	0	Niet getest - handmatig
8. Bestandsupload en rapporten	10	0	0	0	Niet getest - handmatig
9. AI / LLM (OWASP LLM Top 10 2025)	30	0	0	0	Niet getest - handmatig
10. Mobiele app (OWASP MASVS)	34	0	0	0	Buiten scope
11. Windows-desktopapplicatie	27	0	0	0	Buiten scope
12. Telegram-bot en mini-app	24	0	0	0	Niet getest - handmatig
13. Vertrouwen tussen componenten	23	1	1	0	Deels getest
14. Betalingen en facturatie	6	0	0	0	Niet getest - handmatig
15. Supply chain, CI/CD en code	25	1	0	1	Deels getest
16. Logging, monitoring en detectie	10	0	0	0	Niet getest - handmatig
17. Back-up, continuïteit en incidentrespons	11	0	0	0	Niet getest - handmatig
18. Privacy en wettelijke naleving	11	0	0	0	Niet getest - handmatig
19. Beveiligingstesten en kwetsbaarheidsmelding	13	1	0	1	Deels getest
20. Go-live-checklist	17	0	0	0	Niet getest - handmatig

Niet getest / handmatige beoordeling nodig

De volgende onderdelen zijn niet automatisch getest. DPOne kan op verzoek een handmatige beoordeling regelen (info@dpone.info).

- 0. Governance, dreigingsmodel en autorisatie: Architectuur- en datastroomdiagram, STRIDE-dreigingsmodel, classificatie van assets, beleid, verzekering.
- 1. Infrastructuur, netwerk, DNS en TLS: Firewall en open poorten, blootstelling origin-IP, TLS-protocollen/ciphers, servers, containers, cloud-IAM, registrar-lock en 2FA.
- 2. Backend en API: Geauthenticeerde API-tests: injectie, SSRF, IDOR/BOLA, mass assignment, bedrijfslogica, GraphQL/WebSocket, race conditions.
- 3. Authenticatie en sessiebeheer: Wachtwoordbeleid, MFA, wachtwoordherstel, JWT/refresh tokens, OAuth state/PKCE, session fixation (testaccounts nodig).
- 4. Autorisatie en toegangscontrole: Horizontale/verticale privilege-escalatie en tenant-isolatie (twee testaccounts nodig).
- 5. Front-end en publieke website: DOM-XSS, postMessage, CSRF op geauthenticeerde formulieren, tokens in client-opslag, CAPTCHA-omzeiling.
- 6. Dashboards (klant en beheer): Encoding van bevindingen, ondertekende downloads, CSV-injectie, auditlog, impersonatie, vier-ogenprincipe.
- 7. Data, cryptografie en secrets: Versleuteling at rest, sleutelbeheer/KMS, databasehardening, secret-scan van Git-historie.
- 8. Bestandsupload en rapporten: Uploadvalidatie, malwarescan, SVG/ZIP, HTML-naar-PDF SSRF (geauthenticeerd testen

nodig).

- 9. AI / LLM (OWASP LLM Top 10 2025): Volledige red-teaming (jailbreaks), RAG-tenantisolatie, excessive agency, outputverwerking, kostenlimieten.
- 12. Telegram-bot en mini-app: Webhook-secret, initData-validatie, commando-autorisatie, callback_data-IDOR (bottoegang nodig).
- 13. Vertrouwen tussen componenten: Token-audiences per kanaal, service-to-service-authenticatie, webhook-handtekeningen, integratiematrix.
- 14. Betalingen en facturatie: Prijsberekening server-side, activatie via webhook, idempotentie, factuur-IDOR (test-checkout nodig).
- 15. Supply chain, CI/CD en code: Repositorybeveiliging, SAST, secret scanning, SBOM, CI-secrets en runners.
- 16. Logging, monitoring en detectie: Security-logging, SIEM, alerting (interne toegang nodig).
- 17. Back-up, continuïteit en incidentrespons: 3-2-1-back-ups, hersteltests, incidentresponsplan (documentreview).
- 18. Privacy en wettelijke naleving: AVG-documentatie, verwerkersovereenkomst, DPIA, NIS2/AI Act/CRA (via DPOne's AVG-diensten).
- 19. Beveiligingstesten en kwetsbaarheidsmelding: Onafhankelijke handmatige pentest, bug bounty, red teaming, personeelsbeveiliging.
- 20. Go-live-checklist: Portscan, MFA voor beheerders, IDOR-tests, back-ups, incidentplan, externe pentest.

VOORBEELD - GEEN ECHTE BEOORDELING

Bijlage A - Referenties

- 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

VOORBEELD - GEEN ECHTE BEOORDELING

Bijlage B - Begrippenlijst in gewone taal

Penetratietest
Een gecontroleerde test van uw systemen, op uw verzoek, om zwakke plekken te vinden voordat aanvallers dat doen.

Bevinding
Een gevonden zwakheid, met bewijs en een oplossing.

Ernst
Hoe erg een zwakheid is: kritiek, hoog, gemiddeld, laag of informatief.

CVSS
Een internationale score (0 tot 10) voor hoe ernstig een type zwakheid is.

CVE
Een openbaar nummer voor een bekende beveiligingsfout, zoals CVE-2024-1234.

CWE
Een catalogusnaam voor een soort fout, zoals 'cross-site scripting' (CWE-79).

HTTPS / TLS
Het slotje: het versleutelt verkeer tussen bezoekers en uw site.

HSTS
Een regel die browsers vertelt altijd de beveiligde versie van uw site te gebruiken.

Security headers
Kleine instructies die uw site aan browsers stuurt om aanvallen te blokkeren.

SPF, DKIM, DMARC
E-mailinstellingen die voorkomen dat criminelen mail namens u versturen.

DNSSEC
Een digitaal zegel op het adresboek van uw domein, zodat niemand bezoekers kan omleiden.

XSS
Een truc waarbij een aanvaller zijn script in uw pagina laat draaien.

Open redirect
Een link op uw site die mensen naar elke andere site kan sturen, handig voor phishing.

Statische analyse
De bestanden van een app lezen zonder de app uit te voeren.

Remediatie
De oplossing.

Disclaimer

Dit rapport is een momentopname. Het geeft de toestand van het doel op de testdata weer.

Het is beperkt tot de afgesproken scope en tot geautomatiseerde, niet-destructieve controles, tenzij anders vermeld. Het ontbreken van een bevinding bewijst niet dat er geen kwetsbaarheden zijn. Onderdelen gemarkeerd als 'niet getest' zijn niet beoordeeld.

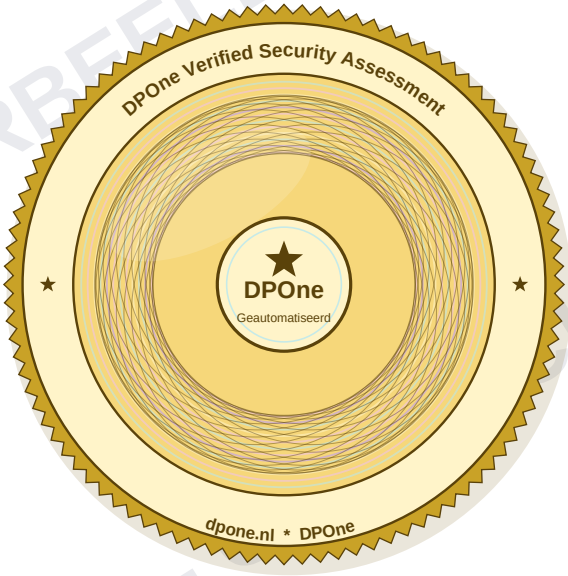
Voor dit rapport heeft geen menselijke pentester handmatige exploitatie uitgevoerd, tenzij uitdrukkelijk vermeld. Het rapport is geen certificering of juridisch advies.

VOORBEELD - GEEN ECHTE BEOORDELING

Ondertekening

Dit rapport is opgesteld door DPOne's geautomatiseerde beoordelingsengine onder de hierboven beschreven autorisatie en uitgegeven door DPOne (MBZ Compliance).

Uitgegeven door	DPOne - MBZ Compliance, Rotterdam, Nederland (KvK 98446932)
Rapport-ID	ptsample00000000000
Uitgegeven	2 november 2026
Doel	example.com
Vingerafdruk resultaten (SHA-256)	SAMPLE-NOT-A-REAL-FINGERPRINT



DPOne Verified Security Assessment

Geautomatiseerd · Niet-destructief · Geautoriseerd

Controleer de echtheid van dit rapport:
https://dpone.nl/verify/ptsample00000000000

VOORBEELD - GEEN ECHTE BEOORDELING