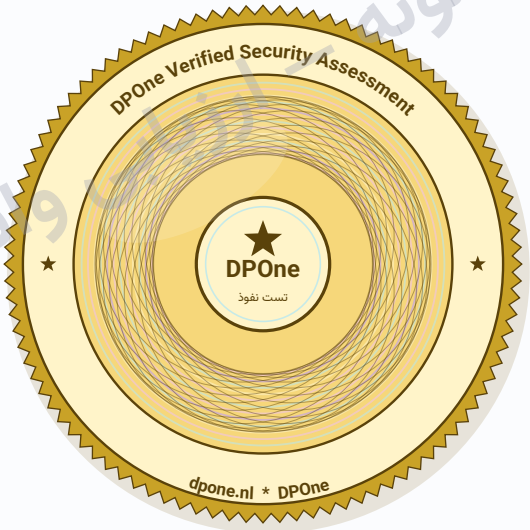
کاملاً محرمانه

گزارش تست نفوذ

ارزیابی امنیتی خودکار و غیرمخرب

example.com



نمونه — ارزیابی واقعی نیست

مشتری	**Example B.V. (SAMPLE)**
هدف	**example.com**
بازه تست	**۱۱ آبان ۱۴۰۵ – ۱۱ آبان ۱۴۰۵**
تاریخ صدور	**۱۱ آبان ۱۴۰۵**
شناسه گزارش	**ptsample00000000000**
افزونه ها	**-**

نمونه — ارزیابی واقعی نیست

کنترل سند

شناسه گزارش	ptsample00000000000
نسخه	۱٫۰ — نهایی
تهیه شده برای	Example B.V. (SAMPLE) — example.com
تهیه کننده	دی پی وان — MBZ Compliance، روتردام، هلند (KvK 98446932)
تاریخ صدور	۱۱ آبان ۱۴۰۵
طبقه بندی	کاملاً محرمانه — شامل ضعف های امنیتی رفع نشده است.
توزیع	فقط افراد مجاز مشتری. بدون اجازه مشتری ارسال نشود.
اثر انگشت نتایج (SHA-256)	SAMPLE-NOT-A-REAL-FINGERPRINT
Engine	DPOne automated engine pentest-1.0.0

جزئیات فنی یافته ها (عنوان، شواهد و راه حل) به انگلیسی آمده تا دقیقاً با استانداردهای بین المللی مطابقت داشته باشد.

فهرست

۱. خلاصه مدیریتی ۳
۲. محدوده و مجوز ۴
۳. روش شناسی ۵
۴. خلاصه یافته ها ۶
۵. شرح یافته ها ۷
۶. نقشه راه رفع ۱۱
۷. ماتریس پوشش چک لیست ۱۲
۸. پیوست الف — مراجع ۱۴
۹. پیوست ب — واژه نامه به زبان ساده ۱۵
۱۰. سلب مسئولیت ۱۵
۱۱. تأیید و امضا ۱۶

نمونه — ارزیابی واقعی نیست

خلاصه مدیریتی

دی پی وان یک ارزیابی امنیتی خودکار و غیرمخرب روی example.com برای Example B.V. (SAMPLE) انجام داد. در محدوده توافق شده ۱۵ بررسی اجرا شد. ۶ یافته نیاز به رسیدگی دارد؛ امتیاز کلی امنیت ۷۰ از ۱۰۰ است.

ریسک کلی
متوسط

امتیاز امنیت
۷۰/۱۰۰

یافته ها بر اساس شدت



مهم ترین یافته ها

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

نقاط قوت

- 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

نمونه — ارزیابی واقعی نیست

محدوده و مجوز

این ارزیابی هدف تأییدشده زیر و در صورت خرید، نسخه های آپلودشده اپلیکیشن را پوشش داد.

داخل محدوده

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

خارج از محدوده

سرویس ها و دامنه های شخص ثالث، بخش های نیازمند ورود، حمله منع سرویس، مهندسی اجتماعی، امنیت فیزیکی و هر سیستمی که در محدوده نیامده است.

مجوز کتبی

تست به صورت کتبی توسط Jane Example (CTO، Example B.V.) در تاریخ ۱۰ آبان ۱۴۰۵ برای بازه ۱۱ آبان ۱۴۰۵ تا ۱۸ آبان ۱۴۰۵ مجاز شد. مالکیت دامنه پیش از ارسال هر ترافیک تست تأیید شد.

قواعد تعامل

- فقط تست های غیرمخرب؛ هیچ داده ای تغییر یا حذف نشد.
- بدون حمله منع سرویس، تست بار، حدس رمز یا مهندسی اجتماعی.
- بدون بهره برداری فراتر از اثبات بی خطر (فقط نشانگرهای بی ضرر).
- درخواست های محدودشده با شناسه کاربری قابل شناسایی.
- اپ های آپلودشده فقط به صورت ایستا تحلیل شدند و هرگز اجرا نشدند.

اپلیکیشن های تحلیل شده

هیچ نسخه ای از اپلیکیشن در محدوده نبود.

نمونه — ارزیابی واقعی نیست

روش شناسی

این ارزیابی مراحل PTES و NIST SP 800-115 (برنامه ریزی، کشف، ارزیابی، گزارش) را دنبال می کند و از آزمون های راهنمای OWASP WSTG نسخه ۴٫۲ استفاده می کند که به طور امن و خودکار از اینترنت قابل اجرا هستند.

نتایج به الزامات OWASP ASVS 4.0.3، فهرست OWASP Top 10:2021، شناسه های CWE و برای اپ موبایل به OWASP MASVS v2 و MASTG نگاشت شده اند. آسیب پذیری های شناخته شده با GitHub Security Advisories، OSV، CISA KEV، NVD و داده های retire.js که روزانه به روز می شوند مقایسه می شوند.

برنامه تست از چک لیست ۲۱ بخشی تست نفوذ دی پی وان (۴۵۸ مورد) پیروی می کند. ماتریس پوشش نشان می دهد کدام بخش ها خودکار تست شده اند و کدام نیاز به بازبینی دستی دارند.

استانداردها

- 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)

شدت و امتیازدهی

شدت، رتبه بندی زمینه ای دی پی وان برای این هدف است. امتیاز پایه CVSS v3.1 شدت عمومی این نوع ضعف را نشان می دهد (بردار برای شفافیت آمده است). امتیاز امنیت از ۱۰۰ شروع می شود و برای هر یافته بحرانی/زیاد/متوسط/کم به ترتیب ۲۵/۱۵/۷/۳ امتیاز کم می شود.

شدت	اثر
بحرانی	با تلاش کم می تواند به نفوذ کامل به دارایی یا داده های آن منجر شود.
زیاد	می تواند به افشای جدی داده یا تصاحب حساب یا سیستم منجر شود.
متوسط	دفاع را ضعیف می کند و همراه با مشکلات دیگر می تواند آسیب بزند.
کم	ضعف جزئی یا کمبود سخت سازی؛ ریسک مستقیم کم.
اطلاعاتی	مشاهده اطلاعاتی؛ بدون ریسک مستقیم.

نمونه — ارزیابی واقعی نیست

خلاصه یافته ها

شناسه	یافته	شدت	دارایی	CVSS	اولویت
F-01	No Content-Security-Policy header	متوسط	example.com	۴.۷	P2
F-02	Vulnerable library: jQuery 3.4.1	متوسط	example.com	۴.۷	P2
F-03	HSTS header missing	متوسط	example.com	۳.۷	P2
F-04	Clickjacking protection missing	کم	example.com	۴.۳	P3
F-05	DMARC policy is p=none	کم	example.com	۴.۳	P3
F-06	No security.txt published	کم	example.com	-	P3

نمونه — ارزیابی واقعی نیست

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

شرح یافته ها

F-01 No Content-Security-Policy header

شدت	متوسط (P2)
CVSS v3.1	۴.۷ — CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N
دارایی آسیب دیده	example.com
دسته	Security headers
بخش چک لیست	۵.۱

شواهد (پاک سازی شده)

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

اثر

دفاع را ضعیف می کند و همراه با مشکلات دیگر می تواند آسیب بزند.

راه حل

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.

مراجع

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

وضعیت بازتست	Open — free automated retest available for 30 days

F-02 Vulnerable library: jQuery 3.4.1

شدت	متوسط (P2)
CVSS v3.1	۴.۷ — CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N
دارایی آسیب دیده	example.com
دسته	Third-party JavaScript
بخش چک لیست	۱۵.۲

شواهد (پاک سازی شده)

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.

اثر

دفاع را ضعیف می کند و همراه با مشکلات دیگر می تواند آسیب بزند.

راه حل

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.

مراجع

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

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

وضعیت بازتست	Open — free automated retest available for 30 days

F-03 HSTS header missing

شدت	متوسط (P2)
CVSS v3.1	۳.۷ — CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N
دارایی آسیب دیده	example.com
دسته	TLS
بخش چک لیست	۱.۲

شواهد (پاک سازی شده)

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

اثر

دفاع را ضعیف می کند و همراه با مشکلات دیگر می تواند آسیب بزند.

راه حل

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

مراجع

/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

وضعیت بازتست	Open — free automated retest available for 30 days

F-04 Clickjacking protection missing

شدت	کم (P3)
CVSS v3.1	۴.۳ — CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
دارایی آسیب دیده	example.com
دسته	Security headers
بخش چک لیست	۵.۱

شواهد (پاک سازی شده)

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

اثر

ضعف جزئی یا کمبود سخت سازی؛ ریسک مستقیم کم.

راه حل

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

مراجع

/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

وضعیت بازتست	Open — free automated retest available for 30 days

F-05 DMARC policy is p=none

شدت	کم (P3)
CVSS v3.1	۴.۳ — CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
دارایی آسیب دیده	example.com
دسته	Email security
بخش چک لیست	۱.۱

شواهد (پاک سازی شده)

```
"dmarc.example.com TXT "v=DMARC1; p=none_
```

اثر

ضعف جزئی یا کمبود سخت سازی؛ ریسک مستقیم کم.

راه حل

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.

مراجع

- 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

وضعیت بازتست Open — free automated retest available for 30 days

F-06 No security.txt published

شدت	کم (P3)
دارایی آسیب دیده	example.com
دسته	Disclosure
بخش چک لیست	۱۹

شواهد (پاک سازی شده)

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

اثر

ضعف جزئی یا کمبود سخت سازی؛ ریسک مستقیم کم.

راه حل

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.

مراجع

- 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

وضعیت بازتست Open — free automated retest available for 30 days

نمونه — ارزیابی واقعی نیست

مشاهدات (اطلاعاتی)

شناسه	یافته	شواهد (پاک سازی شده)
O-01	robots.txt reviewed	.robots.txt lists /admin/ (path exists, login required)

کنترل های تأییدشده

بررسی های زیر موفق بودند:

یافته	دارایی
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

نمونه — ارزیابی واقعی نیست

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

نقشه راه رفع

اولویت			شناسه
P1	ظرف ۷ روز	یافته های بحرانی و زیاد	-
P2	ظرف ۳۰ روز	یافته های متوسط	F-01, F-02, F-03
P3	ظرف ۹۰ روز	یافته های کم و سخت سازی	F-04, F-05, F-06
P4	برنامه ریزی شده	مشاهدات و موارد بازبینی دستی	1 (see coverage) observations + manual review items

P2 — ظرف ۳۰ روز

- 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 — ظرف ۹۰ روز

- 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.

نمونه — ارزیابی واقعی نیست

ماتریس پوشش چک لیست

بررسی های خودکار بخش هایی از هر قسمت را پوشش می دهند که بدون اطلاعات ورود و به طور امن از بیرون قابل تست هستند. موارد پوشش داده نشده برای بازبینی دستی علامت خورده اند.

بخش	موارد	بررسی ها	موفق	ناموفق	وضعیت
۰. حاکمیت، مدل تهدید و مجوز	۲۱	۰	۰	۰	تست بخشی
۱. زیرساخت، شبکه، DNS و TLS	۴۶	۵	۳	۲	تست بخشی
۲. بک اند و API	۴۲	۰	۰	۰	تست نشده – بازبینی دستی
۳. احراز هویت و مدیریت نشست	۲۹	۱	۱	۰	تست بخشی
۴. مجوزدهی و کنترل دسترسی	۱۰	۰	۰	۰	تست نشده – بازبینی دستی
۵. فرانت اند و وب سایت عمومی	۳۸	۶	۳	۲	تست بخشی
۶. داشبوردها (مشتری و ادمین)	۱۳	۰	۰	۰	تست نشده – بازبینی دستی
۷. داده، رمزنگاری و اسرار	۱۸	۰	۰	۰	تست نشده – بازبینی دستی
۸. آپلود فایل و گزارش ها	۱۰	۰	۰	۰	تست نشده – بازبینی دستی
۹. هوش مصنوعی / LLM (OWASP LLM Top 10 2025)	۳۰	۰	۰	۰	تست نشده – بازبینی دستی
۱۰. اپلیکیشن موبایل (OWASP MASVS)	۳۴	۰	۰	۰	خارج از محدوده
۱۱. اپلیکیشن ویندوز	۲۷	۰	۰	۰	خارج از محدوده
۱۲. ربات تلگرام و مینی اپ	۲۴	۰	۰	۰	تست نشده – بازبینی دستی
۱۳. ارتباط و اعتماد بین اجزا	۲۳	۱	۱	۰	تست بخشی
۱۴. پرداخت و صورتحساب	۶	۰	۰	۰	تست نشده – بازبینی دستی
۱۵. زنجیره تأمین، CI/CD و کد	۲۵	۱	۰	۱	تست بخشی
۱۶. لاگ، مانیتورینگ و تشخیص	۱۰	۰	۰	۰	تست نشده – بازبینی دستی
۱۷. پشتیبان گیری، تداوم و پاسخ به حادثه	۱۱	۰	۰	۰	تست نشده – بازبینی دستی
۱۸. حریم خصوصی و انطباق قانونی	۱۱	۰	۰	۰	تست نشده – بازبینی دستی
۱۹. تست امنیتی و برنامه افشای آسیب پذیری	۱۳	۱	۰	۱	تست بخشی
۲۰. چک نهایی قبل از لانچ	۱۷	۰	۰	۰	تست نشده – بازبینی دستی

تست نشده / نیازمند بازبینی دستی

موارد زیر به صورت خودکار تست نشده اند. دی پی وان در صورت درخواست بازبینی دستی را هماهنگ می کند (info@dpone.info).

- ۰. حاکمیت، مدل تهدید و مجوز: نمودار معماری و جریان داده، مدل تهدید STRIDE، طبقه بندی دارایی ها، سیاست ها، بیمه.
- ۱. زیرساخت، شبکه، DNS و TLS: فایروال و پورت های باز، افشای IP اصلی، فهرست پروتکل ها و Cipherهای TLS، سرورها، کانتینرها، IAM ابری، قفل رجیسترار و 2FA.
- ۲. بک اند و API: تست API با احراز هویت: تزریق، Mass Assignment، IDOR/BOLA، SSRF، منطق کسب وکار، Race Condition، GraphQL/WebSocket.
- ۳. احراز هویت و مدیریت نشست: سیاست رمز، MFA، بازیابی رمز، JWT و state/PKCE، Refresh Token در Session Fixation، OAuth (نیازمند حساب تست).
- ۴. مجوزدهی و کنترل دسترسی: ارتقای دسترسی افقی و عمودی و جداسازی تننت ها (نیازمند دو حساب تست).
- ۵. فرانت اند و وب سایت عمومی: CSRF، postMessage، DOM XSS در فرم های دارای احراز هویت، ذخیره توکن سمت کلاینت، دور زدن CAPTCHA.
- ۶. داشبوردها (مشتری و ادمین): Encode یافته ها، لینک دانلود امضاشده، CSV Injection، لاگ ممیزی، Impersonation، تأیید دونفره.
- ۷. داده، رمزنگاری و اسرار: رمزنگاری در حالت سکون، مدیریت کلید/KMS، سخت سازی دیتابیس، اسکن اسرار تاریخچه Git.
- ۸. آپلود فایل و گزارش ها: اعتبارسنجی آپلود، اسکن بدافزار، SVG و ZIP، SSRF در تولید PDF (نیازمند تست با احراز هویت).
- ۹. هوش مصنوعی / Red Team (OWASP LLM Top 10 2025): LLM کامل (Jailbreak)، جداسازی RAG، اختیار بیش از حد ایجنت، مدیریت خروجی، سقف هزینه.
- ۱۲. ربات تلگرام و مینی اپ: Secret وب هوک، اعتبارسنجی initData، مجوز دستورات، IDOR در callback_data (نیازمند دسترسی به ربات).

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

- ۱۳. ارتباط و اعتماد بین اجزا: Audience توکن برای هر کانال، احراز هویت سرویس به سرویس، امضای وب هوک، ماتریس تست یکپارچگی.
- ۱۴. پرداخت و صورتحساب: محاسبه قیمت سمت سرور، فعال سازی فقط با وب هوک، IDOR، Idempotency فاکتور (نیازمند پرداخت آزمایشی).
- ۱۵. زنجیره تأمین، CI/CD و کد: محافظت مخزن، SAST، اسکن اسرار، SBOM، اسرار و Runnerهای CI.
- ۱۶. لاگ، مانیتورینگ و تشخیص: لاگ رویدادهای امنیتی، SIEM، هشدار (نیازمند دسترسی داخلی).
- ۱۷. پشتیبان گیری، تداوم و پاسخ به حادثه: بکاپ ۳-۲-۱، تست بازیابی، طرح پاسخ به حادثه (بازبینی مستندات).
- ۱۸. حریم خصوصی و انطباق قانونی: مستندات NIS2/AI Act/CRA، DPIA، DPA، GDPR (در سرویس های GDPR دی پی وان).
- ۱۹. تست امنیتی و برنامه افشای آسیب پذیری: پن تست دستی مستقل، باگ بانتی، Red Team، امنیت کارکنان.
- ۲۰. چک نهایی قبل از لانچ: اسکن پورت، MFA ادمین ها، تست IDOR، بکاپ، طرح حادثه، پن تست شخص ثالث.

نمونه — ارزیابی واقعی نیست

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

پیوست الف — مراجع

- /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

نمونه — ارزیابی واقعی نیست

پیوست ب — واژه نامه به زبان ساده

تست نفوذ
بررسی کنترل شده سیستم های شما به درخواست خودتان، برای پیدا کردن نقاط ضعف قبل از مهاجمان.

یافته
ضعفی که پیدا کردیم، همراه با شواهد و راه حل.

شدت
میزان خطر یک ضعف: بحرانی، زیاد، متوسط، کم یا اطلاعاتی.

CVSS
یک سیستم امتیازدهی بین المللی (۰ تا ۱۰) برای جدی بودن یک نوع ضعف.

CVE
شماره عمومی یک باگ امنیتی شناخته شده در یک محصول، مثل CVE-2024-1234.

CWE
نام یک نوع اشتباه در کاتالوگ، مثل اسکریپت نویسی بین سایتی (CWE-79).

HTTPS / TLS
همان قفل مرورگر: ترافیک بین بازدیدکننده و سایت را رمز می کند.

HSTS
قانونی که به مرورگر می گوید همیشه نسخه امن سایت را باز کند.

هدرهای امنیتی
دستورهای کوچکی که سایت به مرورگر می فرستد تا حمله های رایج را ببندد.

SPF، DKIM و DMARC
تنظیمات ایمیل که جلوی ارسال ایمیل جعلی به نام شما را می گیرد.

DNSSEC
مهر دیجیتال روی دفترچه آدرس دامنه تا کسی نتواند بازدیدکننده ها را منحرف کند.

XSS
ترفندی که مهاجم اسکریپت خودش را داخل صفحه شما اجرا می کند.

Open Redirect
لینکی در سایت شما که می تواند افراد را به هر سایت دیگری بفرستد؛ مناسب فیشینگ.

تحلیل ایستا
خواندن فایل های اپ بدون اجرا کردن آن.

رفع
همان راه حل.

سلب مسئولیت

این گزارش ارزیابی یک لحظه مشخص است و فقط وضعیت هدف در تاریخ های تست را نشان می دهد.

این گزارش به محدوده توافق شده و بررسی های خودکار و غیرمخرب محدود است، مگر خلاف آن ذکر شده باشد. نبودِ یک یافته به معنی نبودِ آسیب پذیری نیست. مواردی که «تست نشده» علامت خورده اند ارزیابی نشده اند.

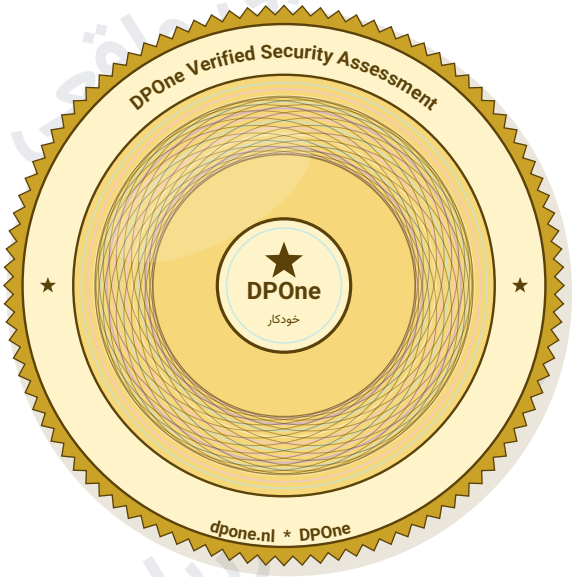
برای این گزارش هیچ تستر انسانی بهره برداری دستی انجام نداده است، مگر صریحاً ذکر شده باشد. این گزارش گواهی نامه یا مشاوره حقوقی نیست.

نمونه — ارزیابی واقعی نیست

تأیید و امضا

این گزارش توسط موتور ارزیابی خودکار دی پی وان و بر اساس مجوز شرح داده شده تهیه و توسط دی پی وان (MBZ Compliance) صادر شده است.

صادرکننده	دی پی وان — MBZ Compliance، روتردام، هلند (KvK 98446932)
شناسه گزارش	ptsample00000000000
تاریخ صدور	۱۱ آبان ۱۴۰۵
هدف	example.com
اثر انگشت نتایج (SHA-256)	SAMPLE-NOT-A-REAL-FINGERPRINT



DPOne Verified Security Assessment

خودکار · غیرمخرب · مجاز

اصالت این گزارش را بررسی کنید:
https://dpone.nl/verify/ptsample00000000000

نمونه — ارزیابی واقعی نیست