IP / 2026-11-03 / فعال + فعال / [redacted]
شناسه اسکن / مدت زمان 428.3 ثانیه
https://salisec.ir

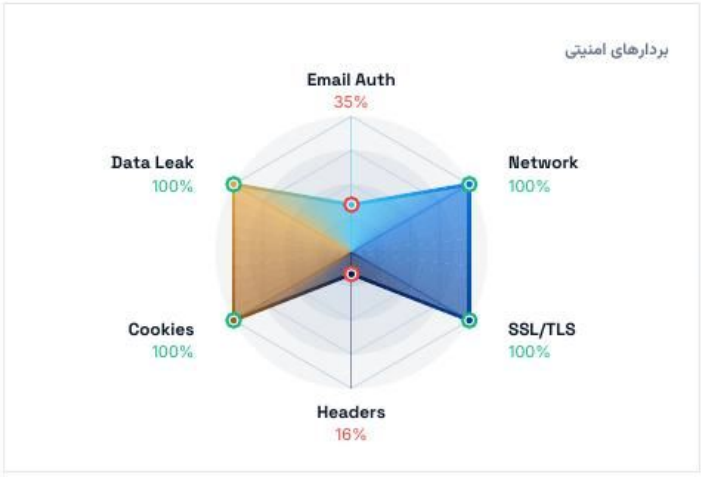
امتیاز امنیتی	ضعف‌ها	تاییدشده / مشاهده‌شده	بررسی‌های تکمیل‌شده	روند نسبت به قبل
49 /100	15	9	100%	+0
مواجهه بالا	بحرانی 1 / زیاد 3 / متوسط 8 / کم 3	6 نشانه‌ی تاییدنشده برای اعتبارسنجی	39 از 39 ماژول، 0 تکمیل‌نشده	2026/11/01 (همان مجموعه‌ی تست) نسبت به امتیاز 49 از 100 در تاریخ

01 خلاصه اجرایی

9 ضعف تاییدشده یا مشاهده‌شده و 6 نشانه‌ی تاییدنشده شناسایی شد. این امتیاز شامل نشانه‌های تاییدنشده است و پس از بررسی دستی ممکن است تغییر کند.

حوزه کنترل	وضعیت	خلاصه یافته	مبنای مدرک
ترابری و TLS	قبول	فقط TLS مدرن، گواهی تا 165 روز دیگر معتبر است	TLSv1.3 / TLS_AES_256_GCM_SHA384
احراز هویت ایمیل	ریسک	اعمال نشده است: امکان جعل این دامنه وجود دارد DMARC	SPF: VALID
هدرهای امنیتی وب	ریسک	5 از 6 هدر امنیتی مشاهده‌شده غایب است	غایب: HSTS, CSP, X-Frame, X-Content, Referrer
سرویس‌های شبکه در معرض دید	قبول	از میان 9 پورت بررسی‌شده، هیچ سرویس در دسترس یافت نشد	پروب TCP محدود روی پورت‌های متداول از پیش تعریف‌شده
مدیریت ورودی (تزریق)	نیازمند تایید	4 نشانه نیازمند بررسی دستی است	ماژول تکمیل نشد (completed/skipped)؛ نتایج قطعی نیستند
شناسایی سطح حمله	اطلاعاتی	400 نقطه پایانی / 8 زیردامنه / 115 فرم	100 صفحه خزش‌شده / 2 فایل JS / 0 مشخصه API

02 چشم‌انداز ریسک







ماتریس ریسک



نشانگر تویر = تاییدشده یا مشاهده‌شده. نشانگر توخالی = نشانه‌ی تاییدنشده. ناحیه‌ی سایه‌دار = مدرک قوی و شدت بالا.

توزیع OWASP Top 10 (2021)

A01 کنترل دسترسی ناقص	A02 نقص‌های رمزنگاری	A03 تزریق	A04 طراحی ناامن	A05 پیکربندی نادرست امنیتی
1 یافته	0 یافته	4 یافته	0 یافته	6 یافته
A06 مولفه‌های آسیب‌پذیر	**A07 نقص‌های احراز هویت**	**A08 نقص‌های یکپارچگی**	**A09 نقص‌های ثبت رویداد**	**A10 SSRF**
0 یافته	2 یافته	0 یافته	0 یافته	1 یافته

خانه‌های خالی به‌معنای نبود یافته است. این امر دسته را «سالم» گواهی نمی‌کند؛ بخش 15 موارد تست‌شده را فهرست می‌کند.

03 یافته‌های اولویت‌دار (5 مورد برتر)

چه اتفاقی می‌تواند بیفتد

در صورت تایید، مهاجم می‌تواند کنترل سایت را در دست بگیرد، بیشتر داده‌های آن را سرقت کند یا بخش‌های کلیدی آن را از کار بیندازد.

نیازمند بررسی 65.3 ریسک / بحرانی / P2

نشانه‌ی SSTI روی پارامتر 'cat' در /

تاثیر: رفتار پاسخ نشان می‌دهد که پارامتر 'cat' ممکن است بدون پاکسازی مناسب، روی یک کوئری/قالب SSTI در بک‌اند تاثیر بگذارد

/ دارایی / active / NOT VERIFIED / LOW اطمینان / CVSS 9.3

- نقطه پایانی

A03:2021 - Injection / WSTG-INPV-11 / ASVS V5.3.4

چه اتفاقی می‌تواند بیفتد

در صورت تایید، مهاجم می‌تواند به داده‌های مهم دسترسی پیدا کند یا آن‌ها را تغییر دهد، یا بخش‌هایی از سایت را مختل کند.

نیازمند بررسی 57.2 ریسک / زیاد / P2

نشانه‌ی NoSQLi روی پارامتر 'cat' در /

تاثیر: رفتار پاسخ نشان می‌دهد که پارامتر 'cat' ممکن است بدون پاکسازی مناسب، روی یک کوئری/قالب NoSQLi در بک‌اند تاثیر بگذارد

/ دارایی / active / NOT VERIFIED / LOW اطمینان / CVSS 8.6

- نقطه پایانی

A03:2021 - Injection / WSTG-INPV-05 / ASVS V5.3.4

چه اتفاقی می‌تواند بیفتد

در صورت تایید، مهاجم می‌تواند به داده‌های مهم دسترسی پیدا کند یا آن‌ها را تغییر دهد، یا بخش‌هایی از سایت را مختل کند.

نیازمند بررسی 54.0 ریسک / زیاد / P3

نشانه‌ی SQLi روی پارامتر 'cat' در /

تاثیر: رفتار پاسخ نشان می‌دهد که پارامتر 'cat' ممکن است بدون پاکسازی مناسب، روی یک کوئری/قالب SQLi در بک‌اند تاثیر بگذارد

/ دارایی / active / NOT VERIFIED / LOW اطمینان / CVSS 8.6

- نقطه پایانی

A03:2021 - Injection / WSTG-INPV-05 / ASVS V5.3.4

چه اتفاقی می‌تواند بیفتد

حملات دیگر را آسان‌تر می‌کند یا می‌تواند برخی اطلاعات را افشا کند.

تاییدشده / مشاهده‌شده 49.2 ریسک / متوسط / P3

سیاست DMARC ضعیف است یا تعریف نشده (MISSING)

تاثیر: امکان جعل ایمیل و فیشینگ با استفاده از دامنه‌ی هدف را فراهم می‌کند

/ دارایی / passive / MEDIUM اطمینان / CVSS 6.2

- نقطه پایانی

A07:2021 - Identification and Authentication Failures

چه اتفاقی می‌تواند بیفتد

در صورت تایید، مهاجم می‌تواند به داده‌های مهم دسترسی پیدا کند یا آن‌ها را تغییر دهد، یا بخش‌هایی از سایت را مختل کند.

نیازمند بررسی 48.3 ریسک / زیاد / P3

نشانه‌ی LDAP روی پارامتر 'cat' در /

تاثیر: رفتار پاسخ نشان می‌دهد که پارامتر 'cat' ممکن است بدون پاکسازی مناسب، روی یک کوئری/قالب LDAP در بک‌اند تاثیر بگذارد

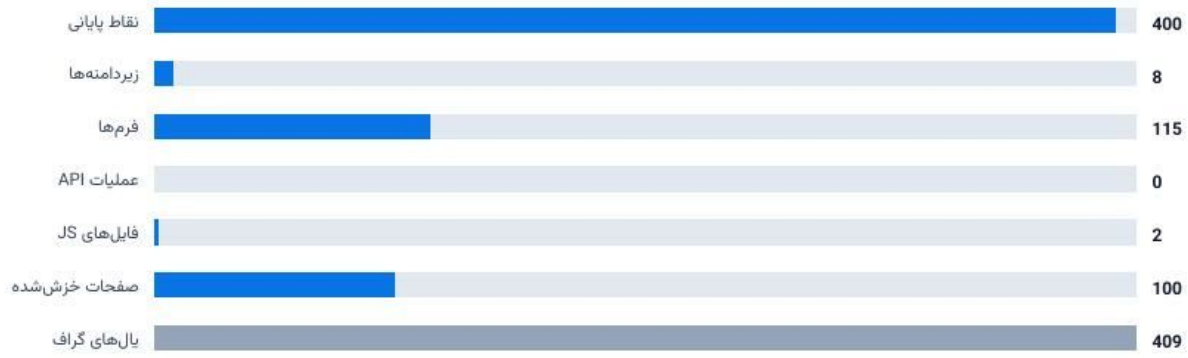
/ دارایی / active / NOT VERIFIED / LOW اطمینان / CVSS 7.7

- نقطه پایانی

A03:2021 - Injection / WSTG-INPV-06 / ASVS V5.3.4

04 فهرست سطح حمله

نقاط پایانی	زیردامنه‌ها	فرم‌ها	عملیات API	فایل‌های JS	صفحات خزش‌شده
400	8	115	0	2	100
کشف‌شده	از لاگ‌های CT	کشف‌شده	از OpenAPI	اسکن‌شده	هم‌مبدا



05 ماتریس کنترل‌های امنیتی

هدرهای امنیتی HTTP

X-Frame: موجود نیست	CSP: موجود نیست	HSTS: موجود نیست
Permissions: موجود	Referrer: موجود نیست	X-Content: موجود نیست

مواجهه‌ی پورت‌های شبکه

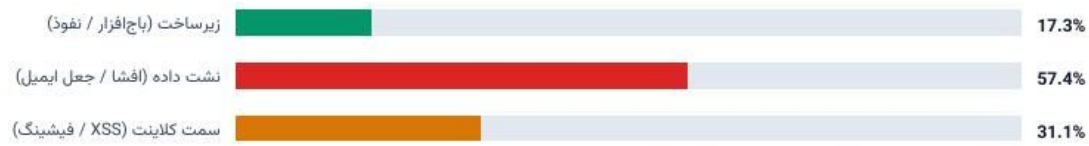
80 HTTP: FILTERED	22 SSH: FILTERED	21 FTP: FILTERED
5432 PostgreSQL: FILTERED	3306 MySQL: FILTERED	443 HTTPS: FILTERED
27017 MongoDB: FILTERED	8080 HTTP-Alt: FILTERED	6379 Redis: FILTERED

کوکی	Secure	HttpOnly	SameSite
چیزی مشاهده نشد	-	-	-

06 وضعیت دارایی‌های حیاتی

گواهی SSL	قدیمی TLS	ریدایرکت HTTPS	ایمیل (DMARC)	افشای دیتابیس	لایه WAF
VALID (165d)	فقط مدرن	ACTIVE	MISSING	محافظت‌شده	شناسایی نشد

07 میزان مواجهه‌ی کسب‌وکار با تهدید (شاخص تقریبی)



این شاخص‌ها خلاصه‌های وزن‌دهی‌شده‌ی یافته‌های بالا هستند، نه احتمال وقوع.

08 تحلیل TLS و گواهی

ویژگی	مقدار
پروتکل مذاکره‌شده	TLSv1.3
مجموعه‌رمز مذاکره‌شده	TLS_AES_256_GCM_SHA384
کلید عمومی گواهی	RSA 2048
الگوریتم امضا	sha256WithRSAEncryption

ویژگی	مقدار
صادرکننده	Certum DV TLS G2 R39 CA
خودامضا	خیر
قدیمی TLS 1.0 / 1.1	خیر (فقط مدرن)
سایفرهای ضعیف TLS	چیزی مشاهده نشد

عمر باقی‌مانده‌ی گواهی



حضور DNSSEC صرفا بررسی حضور DNSKEY است، نه اعتبارسنجی کامل زنجیره‌ی اعتماد تا ریشه.

09 وضعیت امنیتی HTTP

بررسی	نتیجه
سیاست HSTS	ارسال نشد
بازتاب مبدا CORS	اعتبارسنجی نشد (پاسخ HTTPS در دسترس نیست)
محافظت در برابر Clickjacking	محافظتی در برابر clickjacking یافت نشد
متدهای HTTP مجاز	ثبت نشد
نشانه‌های افشای خطا	چیزی مشاهده نشد
بازتاب هدر Host	شناسایی نشد
پارامتر تغییرمسیر باز	هیچ
فهرست دایرکتوری	یافت نشد

10 بازتاب ورودی و آمار تست‌های فعال

پارامترهای تست‌شده	فرم‌های تست‌شده	آزمون‌های اجراشده	آزمون‌های ردشده	آزمون‌های پایان‌مهلت
15	0	71	0	9
پارامتر پرس‌وجو	فرم‌ها	پروب بی‌خطر	اجرا نشد	بدون نتیجه

بازتاب ورودی: بازتاب بدون escape برای نشانه‌ی بی‌خطر آزمایشی یافت نشد.



11 گزارش مدرک فنی و خوداعتبارسنجی

یافته / بررسی	مدرک مشاهده‌شده	دستور اعتبارسنجی
DMARC Record Missing/Weak	DNS TXT Result: No TXT Record found	`dig +short TXT [redacted]`
Missing Security Headers	Absent Headers: Strict-Transport-Security, Content-Security-Policy, X-Frame-Options ...	`curl -sI [redacted] | grep -i 'Strict-Transport-Security'`
CPE Candidate: Wordpress unknown	Detected: Wordpress (version unknown). CPE prefix: cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:*:*:*. Determine exact version and check NVD (https://nvd.nist.gov/vuln/search) or OSV (htt	`# Check NVD: https://nvd.nist.gov/vuln/search?query=wordpress+unknown`

12 سطح حمله‌ی کشف‌شده

مورد	نتیجه
زیردامنه‌ها (CT)	[redacted]
اعتبار IP	پرسش نشد / در دسترس نیست
افشای مسیر حساس	هیچ‌کدام از مسیرهای بررسی‌شده، HTTP 200 برنگرداندند
security.txt	منتشرنشده
فناوری / CMS	WordPress, jQuery, performant-translations 1.2.0
CAA	منتشرنشده
DNSSEC	شناسایی نشد
رکوردهای MX	10 [redacted]

مورد	نتیجه
رکوردهای NS	irns1.netafraz.com, irns2.netafraz.com, ns3.netafraz.com
معکوس PTR	[redacted]
OpenAPI / Swagger	چیزی یافت نشد
غنی‌سازی زنده‌ی CVE (OSV.dev)	(ای بازگردانده نشدCVE هیچ) OSV از 0 پرسش 0 CVE
نامزدهای CPE (یادداشت‌های آفلاین)	1

13 پیوست یافته‌ها

شناسه	اولویت	ریسک	CVSS	شدت	CWE	سطح	اطمینان	وضعیت تایید
SSF-008857346EFFB0744957	P2	65.3	9.3	بحرانی	CWE-1336	active	LOW	NOT VERIFIED
SSF-897017E9FC498103B88D	P2	57.2	8.6	زیاد	CWE-943	active	LOW	NOT VERIFIED
SSF-2FB73877E8A86FB27B0E	P3	54.0	8.6	زیاد	CWE-89	active	LOW	NOT VERIFIED
SSF-95D7B65C7BC150F28477	P3	49.2	6.2	متوسط	CWE-290	passive	MEDIUM	OBSERVED
SSF-7FFF4B131E649F66103E	P3	48.3	7.7	زیاد	CWE-90	active	LOW	NOT VERIFIED
SSF-CC8A5E771674A7832C31	P3	42.3	5.8	متوسط	CWE-693	passive	MEDIUM	OBSERVED
SSF-18DB1906379CCED10037	P4	29.2	4.0	متوسط	CWE-693	passive	MEDIUM	OBSERVED
SSF-2A28AD5CD0FE830F2374	P4	29.2	4.0	متوسط	CWE-693	passive	MEDIUM	OBSERVED
SSF-CB1613F24E777BEED8C6	P4	29.2	4.0	متوسط	CWE-693	passive	MEDIUM	OBSERVED
SSF-957E44C08CB19457D0D8	P4	29.2	4.0	متوسط	CWE-1021	passive	MEDIUM	OBSERVED
SSF-43BD1F87B77F0146F963	P4	27.7	4.9	متوسط	CWE-918	active	LOW	NOT VERIFIED
SSF-E65EB272C8E37436B040	P4	26.9	3.7	کم	CWE-200	passive	LOW	OBSERVED
SSF-C23F474553329138F262	P4	26.4	3.7	کم	CWE-284	passive	MEDIUM	OBSERVED
SSF-C3C52A7F5F7668E97420	P4	25.1	4.0	متوسط	CWE-290	passive	LOW	NOT VERIFIED
SSF-798505D402BF63296660	P4	21.2	2.9	کم	CWE-693	passive	MEDIUM	OBSERVED

شناسه	بردار پایه‌ی CVSS 3.1 (امتیاز از روی همین بردار بازمحاسبه می‌شود)
SSF-008857346EFFB0744957	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N
SSF-897017E9FC498103B88D	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
SSF-2FB73877E8A86FB27B0E	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
SSF-95D7B65C7BC150F28477	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N
SSF-7FFF4B131E649F66103E	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
SSF-CC8A5E771674A7832C31	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
SSF-18DB1906379CCED10037	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N
SSF-2A28AD5CD0FE830F2374	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
SSF-CB1613F24E777BEED8C6	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N
SSF-957E44C08CB19457D0D8	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

شناسه	بردار پایه‌ی CVSS 3.1 (امتیاز از روی همین بردار بازمحاسبه می‌شود)
SSF-43BD1F87B77F0146F963	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:N
SSF-E65EB272C8E37436B040	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
SSF-C23F474553329138F262	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
SSF-C3C52A7F5F7668E97420	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
SSF-798505D402BF63296660	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

14 پرونده‌های مدرک

نیازمند بررسی / CVSS 9.3 / بحرانی / P2	SSF-00885734FEFFB0744957
عنوان	نشانه‌ی SSTI روی پارامتر 'cat' در /
دارایی / نقطه پایانی	- / [redacted]
طبقه‌بندی	CWE CWE-1336 / A03:2021 - Injection / WSTG-INPV-11 / ASVS V5.3.4
اطمینان / منبع	LOW / NOT VERIFIED / injection.ssti / active
تاثیر	رفتار پاسخ نشان می‌دهد که پارامتر 'cat' ممکن است بدون پاکسازی مناسب، روی یک کوئری/قالب SSTI در بک‌اند تاثیر بگذارد
چه اتفاقی می‌تواند بیفتد	در صورت تایید، مهاجم می‌تواند کنترل سایت را در دست بگیرد، بیشتر داده‌های آن را سرقت کند یا بخش‌های کلیدی آن را از کار بیندازد.
مدرک	Response delta (weak signal): status 404->301, length delta 152353b | Response delta (weak signal): status 404->301, length delta 152353b | Response delta (weak signal): status 404->301, length delta 152353b
راه‌حل	از کوئری‌های پارامتری‌شده / یک template engine با auto-escaping استفاده کنید؛ تمام ورودی کاربر را سمت سرور اعتبارسنجی و encode کنید (تلاش: MEDIUM)
محدودیت‌ها	Signature/delta/reflection indicator only — no exploitation attempted, no data accessed or modified

نیازمند بررسی / CVSS 8.6 / زیاد / P2	SSF-897017E9FC498103B88D
عنوان	نشانه‌ی NoSQLi روی پارامتر 'cat' در /
دارایی / نقطه پایانی	- / [redacted]
طبقه‌بندی	CWE CWE-943 / A03:2021 - Injection / WSTG-INPV-05 / ASVS V5.3.4
اطمینان / منبع	LOW / NOT VERIFIED / injection.nosqli / active
تاثیر	رفتار پاسخ نشان می‌دهد که پارامتر 'cat' ممکن است بدون پاکسازی مناسب، روی یک کوئری/قالب NoSQLi در بک‌اند تاثیر بگذارد
چه اتفاقی می‌تواند بیفتد	در صورت تایید، مهاجم می‌تواند به داده‌های مهم دسترسی پیدا کند یا آن‌ها را تغییر دهد، یا بخش‌هایی از سایت را مختل کند.
مدرک	Response delta (weak signal): status 404->301, length delta 152353b | Response delta (weak signal): status 404->200, length delta 109791b
راه‌حل	از کوئری‌های پارامتری‌شده / یک template engine با auto-escaping استفاده کنید؛ تمام ورودی کاربر را سمت سرور اعتبارسنجی و encode کنید (تلاش: MEDIUM)
محدودیت‌ها	Signature/delta/reflection indicator only — no exploitation attempted, no data accessed or modified

نیازمند بررسی / CVSS 8.6 / زیاد / P3	SSF-2FB73877E8A86FB27B0E
عنوان	نشانه‌ی SQLi روی پارامتر 'cat' در /
دارایی / نقطه پایانی	- / [redacted]
طبقه‌بندی	CWE CWE-89 / A03:2021 - Injection / WSTG-INPV-05 / ASVS V5.3.4
اطمینان / منبع	LOW / NOT VERIFIED / injection.sqli / active
تاثیر	رفتار پاسخ نشان می‌دهد که پارامتر 'cat' ممکن است بدون پاکسازی مناسب، روی یک کوئری/قالب SQLi در بک‌اند تاثیر بگذارد
چه اتفاقی می‌تواند بیفتد	در صورت تایید، مهاجم می‌تواند به داده‌های مهم دسترسی پیدا کند یا آن‌ها را تغییر دهد، یا بخش‌هایی از سایت را مختل کند.
مدرک	Response delta (weak signal): status 404->301, length delta 152353b
راه‌حل	از کوئری‌های پارامتری‌شده / یک template engine با auto-escaping استفاده کنید؛ تمام ورودی کاربر را سمت سرور اعتبارسنجی و encode کنید (تلاش: MEDIUM)
محدودیت‌ها	Signature/delta/reflection indicator only — no exploitation attempted, no data accessed or modified

تاییدشده / مشاهده‌شده / CVSS 6.2 / متوسط / P3	SSF-95D7B65C7BC150F28477
عنوان	سیاست DMARC ضعیف است یا تعریف نشده (MISSING)
دارایی / نقطه پایانی	[redacted] / -
طبقه‌بندی	CWE CWE-290 / A07:2021 - Identification and Authentication Failures
اطمینان / منبع	MEDIUM / OBSERVED / dns / passive
تاثیر	امکان جعل ایمیل و فیشینگ با استفاده از دامنه‌ی هدف را فراهم می‌کند
چه اتفاقی می‌تواند بیفتد	حملات دیگر را آسان‌تر می‌کند یا می‌تواند برخی اطلاعات را افشا کند.
مدرک	Generated by module: dns
راه‌حل	سیاست DMARC را روی p=quarantine یا p=reject تنظیم کنید (تلاش: MEDIUM)
محدودیت‌ها	محدودیت خاصی برای این یافته ثبت نشده است.

نیازمند بررسی / CVSS 7.7 / زیاد / P3	SSF-7FFF4B131E649F66103E
عنوان	نشانه‌ی LDAP روی پارامتر 'cat' در /
دارایی / نقطه پایانی	[redacted] / -
طبقه‌بندی	CWE CWE-90 / A03:2021 - Injection / WSTG-INPV-06 / ASVS V5.3.4
اطمینان / منبع	LOW / NOT VERIFIED / injection.ldap / active
تاثیر	رفتار پاسخ نشان می‌دهد که پارامتر 'cat' ممکن است بدون پاکسازی مناسب، روی یک کوئری/قالب LDAP در بک‌اند تاثیر بگذارد
چه اتفاقی می‌تواند بیفتد	در صورت تایید، مهاجم می‌تواند به داده‌های مهم دسترسی پیدا کند یا آن‌ها را تغییر دهد، یا بخش‌هایی از سایت را مختل کند.
مدرک	Response delta (weak signal): status 404->200, length delta 109791b
راه‌حل	از کوئری‌های پارامتری‌شده / یک template engine با auto-escaping استفاده کنید؛ تمام ورودی کاربر را سمت سرور اعتبارسنجی و encode کنید (تلاش: MEDIUM)
محدودیت‌ها	Signature/delta/reflection indicator only — no exploitation attempted, no data accessed or modified

تاییدشده / مشاهده‌شده / CVSS 5.8 / متوسط / P3	SSF-CC8A5E771674A7832C31
عنوان	هدر امنیتی موجود نیست: Content-Security-Policy
دارایی / نقطه پایانی	[redacted] / -
طبقه‌بندی	CWE CWE-693 / A05:2021 - Security Misconfiguration
اطمینان / منبع	MEDIUM / OBSERVED / http / passive
تاثیر	مواجهه با حملات تزریق اسکریپت (XSS) و تزریق داده را افزایش می‌دهد
چه اتفاقی می‌تواند بیفتد	حملات دیگر را آسان‌تر می‌کند یا می‌تواند برخی اطلاعات را افشا کند.
مدرک	Generated by module: http
راه‌حل	وب‌سرور را برای ارسال هدر Content-Security-Policy پیکربندی کنید (تلاش: MEDIUM)
محدودیت‌ها	محدودیت خاصی برای این یافته ثبت نشده است.

تاییدشده / مشاهده‌شده / CVSS 4.0 / متوسط / P4	SSF-18DB1906379CCED10037
عنوان	هدر امنیتی موجود نیست: Strict-Transport-Security
دارایی / نقطه پایانی	[redacted] / -
طبقه‌بندی	CWE CWE-693 / A05:2021 - Security Misconfiguration
اطمینان / منبع	MEDIUM / OBSERVED / http / passive
تاثیر	ممکن است مرورگرها فریب بخورند و از طریق HTTP ساده متصل شوند که امکان حملات downgrade/MITM را فراهم می‌کند
چه اتفاقی می‌تواند بیفتد	حملات دیگر را آسان‌تر می‌کند یا می‌تواند برخی اطلاعات را افشا کند.
مدرک	Generated by module: http
راه‌حل	وب‌سرور را برای ارسال هدر Strict-Transport-Security پیکربندی کنید (تلاش: MEDIUM)
محدودیت‌ها	محدودیت خاصی برای این یافته ثبت نشده است.

تاییدشده / مشاهده‌شده / CVSS 4.0 / متوسط / P4	SSF-2A28AD5CD0FE830F2374
عنوان	هدر امنیتی موجود نیست: X-Frame-Options
دارایی / نقطه پایانی	[redacted] / -
طبقه‌بندی	CWE CWE-693 / A05:2021 - Security Misconfiguration
اطمینان / منبع	MEDIUM / OBSERVED / http / passive
تاثیر	صفحه می‌تواند در یک iframe مخفی جاسازی شود که امکان clickjacking را فراهم می‌کند
چه اتفاقی می‌تواند بیفتد	حملات دیگر را آسان‌تر می‌کند یا می‌تواند برخی اطلاعات را افشا کند.
مدرک	Generated by module: http
راه‌حل	وب‌سرور را برای ارسال هدر X-Frame-Options پیکربندی کنید (تلاش: MEDIUM)
محدودیت‌ها	محدودیت خاصی برای این یافته ثبت نشده است.

تاییدشده / مشاهده‌شده / CVSS 4.0 / متوسط / P4	SSF-CB1613F24E777BEED8C6
عنوان	هدر امنیتی موجود نیست: X-Content-Type-Options
دارایی / نقطه پایانی	[redacted] / -
طبقه‌بندی	CWE CWE-693 / A05:2021 - Security Misconfiguration
اطمینان / منبع	MEDIUM / OBSERVED / http / passive
تاثیر	مرورگر ممکن است پاسخ‌ها را MIME-sniff کند که امکان حملات content-type confusion را فراهم می‌کند
چه اتفاقی می‌تواند بیفتد	حملات دیگر را آسان‌تر می‌کند یا می‌تواند برخی اطلاعات را افشا کند.
مدرک	Generated by module: http
راه‌حل	وب‌سرور را برای ارسال هدر X-Content-Type-Options پیکربندی کنید (تلاش: MEDIUM)
محدودیت‌ها	محدودیت خاصی برای این یافته ثبت نشده است.

تاییدشده / مشاهده‌شده / CVSS 4.0 / متوسط / P4	SSF-957E44C08CB19457D0D8
عنوان	عدم وجود محافظت در برابر Clickjacking (هر دو X-Frame-Options و CSP frame-ancestors غایب‌اند) (X-Frame-Options and CSP frame-ancestors both absent)
دارایی / نقطه پایانی	[redacted] / -
طبقه‌بندی	CWE CWE-1021
اطمینان / منبع	MEDIUM / OBSERVED / http_posture / passive
تاثیر	صفحه می‌تواند در یک iframe مخفی/پنهان‌شده در سایت مهاجم جاسازی شود (clickjacking)
چه اتفاقی می‌تواند بیفتد	حملات دیگر را آسان‌تر می‌کند یا می‌تواند برخی اطلاعات را افشا کند.
مدرک	Generated by module: http_posture
راه‌حل	هدر X-Frame-Options: DENY یا دایرکتیو CSP frame-ancestors را اضافه کنید (تلاش: MEDIUM)
محدودیت‌ها	محدودیت خاصی برای این یافته ثبت نشده است.

نیازمند بررسی / CVSS 4.9 / متوسط / P4	SSF-43BD1F87B77F0146F963
عنوان	پارامتر(های) کاندید احتمالی SSRF (1): url
دارایی / نقطه پایانی	[redacted] / -
طبقه‌بندی	CWE CWE-918 / A10:2021 - Server-Side Request Forgery / WSTG-INPV-19
اطمینان / منبع	LOW / NOT VERIFIED / ssrf.param-name / active
تاثیر	پارامترهایی که مقادیر شبیه URL می‌پذیرند ممکن است یک fetch سمت سرور را فعال کنند؛ می‌تواند برای دسترسی به سرویس‌های داخلی، متادیتای ابر یا اسکن پشت پریمیتر سوءاستفاده شود
چه اتفاقی می‌تواند بیفتد	در صورت تایید، حملات دیگر را آسان‌تر می‌کند یا می‌تواند برخی اطلاعات را افشا کند.
مدرک	Parameter 'url' found at /
راه‌حل	تمام پارامترهای حامل URL را سمت سرور اعتبارسنجی و allow-list کنید؛ محدوده‌های RFC1918/loopback/link-local/متادیتای ابر را مسدود کنید (تلاش: MEDIUM)
محدودیت‌ها	Parameter name match only — no URL was fetched or tested; manual review required

تاییدشده / مشاهده‌شده / CVSS 3.7 / کم / P4	SSF-E65EB272C8E37436B040
عنوان	مسیر(های) ظاهرا حساس را فاش می‌کند robots.txt: /wp-admin/, /wp-admin/admin-ajax.php
دارایی / نقطه پایانی	- / [redacted]
طبقه‌بندی	CWE CWE-200 / A01:2021 - Broken Access Control
اطمینان / منبع	LOW / OBSERVED / robots.txt / passive
تاثیر	مسیرهایی را که اپراتور سعی دارد از خزنده‌ها پنهان کند فاش می‌کند؛ این فقط جنبه‌ی توصیه‌ای دارد robots.txt
چه اتفاقی می‌تواند بیفتد	به‌تنهایی بعید است آسیبی وارد کند، اما به مهاجمان یک مزیت کوچک می‌دهد.
مدرک	Generated by module: robots.txt
راه‌حل	برای پنهان‌کردن مسیرهای حساس به robots.txt متکی نباشید؛ کنترل دسترسی را سمت سرور اعمال کنید (تلاش: MEDIUM)
محدودیت‌ها	Paths were read from robots.txt only; no access attempt was made

تاییدشده / مشاهده‌شده / CVSS 3.7 / کم / P4	SSF-C23F474553329138F262
عنوان	رکورد CAA منتشر نشده است
دارایی / نقطه پایانی	- / [redacted]
طبقه‌بندی	CWE CWE-284 / A05:2021 - Security Misconfiguration
اطمینان / منبع	MEDIUM / OBSERVED / dns_posture / passive
تاثیر	بدون رکورد CAA، هر مرجع صدور گواهی عمومی (CA) می‌تواند برای این دامنه گواهی صادر کند
چه اتفاقی می‌تواند بیفتد	به‌تنهایی بعید است آسیبی وارد کند، اما به مهاجمان یک مزیت کوچک می‌دهد.
مدرک	Generated by module: dns_posture
راه‌حل	یک رکورد CAA منتشر کنید که صدور گواهی را به CA(های) انتخابی شما محدود کند (تلاش: MEDIUM)
محدودیت‌ها	محدودیت خاصی برای این یافته ثبت نشده است.

نیازمند بررسی / CVSS 4.0 / متوسط / P4	SSF-C3C52A7F5F7668E97420
عنوان	رکورد DKIM در selectorهای رایج یافت نشد
دارایی / نقطه پایانی	- / [redacted]
طبقه‌بندی	CWE CWE-290 / A07:2021 - Identification and Authentication Failures
اطمینان / منبع	LOW / NOT VERIFIED / dns.dkim-common-selectors / passive
تاثیر	بدون DKIM، سرورهای دریافت‌کننده‌ی ایمیل نمی‌توانند به‌صورت رمزنگاری‌شده تایید کنند که ایمیل خروجی دست‌کاری یا جعل نشده است
چه اتفاقی می‌تواند بیفتد	در صورت تایید، حملات دیگر را آسان‌تر می‌کند یا می‌تواند برخی اطلاعات را افشا کند.
مدرک	Generated by module: dns.dkim-common-selectors
راه‌حل	یک رکورد TXT مربوط به DKIM برای selector(های) ایمیل خروجی خود منتشر کنید؛ نام دقیق selector را از ارائه‌دهنده‌ی سرویس ایمیل خود بپرسید (تلاش: MEDIUM)
محدودیت‌ها	Only common selector names were probed; a nonstandard selector would not be detected

تاییدشده / مشاهده‌شده / CVSS 2.9 / کم / P4	SSF-798505D402BF63296660
عنوان	هدر امنیتی موجود نیست: Referrer-Policy
دارایی / نقطه پایانی	- / [redacted]
طبقه‌بندی	CWE CWE-693 / A05:2021 - Security Misconfiguration
اطمینان / منبع	MEDIUM / OBSERVED / http / passive
تاثیر	به سایت‌های شخص ثالث افشا شوند Referer های کامل (که احتمالا شامل پارامترهای کوئری حساس هستند) ممکن است از طریق هدرURL
چه اتفاقی می‌تواند بیفتد	به‌تنهایی بعید است آسیبی وارد کند، اما به مهاجمان یک مزیت کوچک می‌دهد.
مدرک	Generated by module: http
راه‌حل	وب‌سرور را برای ارسال هدر Referrer-Policy پیکربندی کنید (تلاش: MEDIUM)
محدودیت‌ها	محدودیت خاصی برای این یافته ثبت نشده است.

15 پوشش، اطمینان و محدودیت‌ها



تکمیل‌شده: 39 ردشده: 0 پایان‌مهلت: 0 ناموفق: 0 سایر: 0

ماژول‌های این مجموعه تست؛ یک ماژول ردشده یا ناقص هرگز سالم گزارش نمی‌شود.

درخواست‌های HTTP		278/1200
پرسش‌های DNS		55/260

سطح	ماژول	بررسی	وضعیت	اطمینان	مدرک	محدودیت
passive	**dns**	dkim-common-selectors	**INCONCLUSIVE**	LOW	No configured common selector responded	Common-selector probing cannot establish that DKIM is absent
passive	**tls_cipher_enum**	weak-cipher	**COMPLETED**	INFORMATIONAL	weak=[]	
active	**waf**	benign-differential-probe	**COMPLETED**	LOW	No WAF signature observed	Absence of a signature does not establish application vulnerability
passive	**csp_directives**	parse	**SKIPPED**	INFORMATIONAL	no CSP header	Nothing to parse
passive	**tech_fingerprint_deep**	signatures	**COMPLETED**	INFORMATIONAL	tech=['WordPress', 'jQuery', 'performant-translations 1.2.0']	
passive	**dns_posture**	dnskey-presence	**INCONCLUSIVE**	LOW	No DNSKEY record observed	DNSKEY presence is not full DNSSEC chain validation
passive	**dns_wildcard**	random-subdomain	**COMPLETED**	INFORMATIONAL	wildcard=False	
passive	**dns_zone_transfer**	axfr	**COMPLETED**	INFORMATIONAL	allowed=False nameservers=3	
passive	**reverse_dns**	ptr	**COMPLETED**	INFORMATIONAL	[redacted] m	
passive	**dns_intelligence**	mx-ns-wordlist	**COMPLETED**	INFORMATIONAL	mx=1 ns=3 subdomains=4	
passive	**robots_sitemap**	fetch	**COMPLETED**	INFORMATIONAL	disallow=17 sitemaps=1	
passive	**well_known**	existence	**COMPLETED**	INFORMATIONAL	present=[]	
passive	**crossdomain**	fetch	**COMPLETED**	INFORMATIONAL	permissive=[]	
active	**crawl_surface**	bounded-bfs	**COMPLETED**	INFORMATIONAL	pages=100 endpoints=407 params=8 js=2 forms=115	
active	**js_intelligence**	scan	**COMPLETED**	INFORMATIONAL	files=2 endpoints=0 secrets=0	
active	**api_discovery**	existence	**COMPLETED**	INFORMATIONAL	surface=0 introspection=False	
active	**openapi_surface**	swagger/openapi JSON	**NOT FOUND**	INFORMATIONAL	bounded JSON candidate paths checked	
active	**websocket_intelligence**	url-discovery	**COMPLETED**	INFORMATIONAL	websocket_endpoints=0	Discovery only; no websocket handshake or message was sent
active	**authorization_candidates**	object-endpoint-discovery	**COMPLETED**	INFORMATIONAL	candidates=0	Candidate discovery only; no cross-account or unauthorized access was attempted
active	**security_misconfig**	dir_listing	**COMPLETED**	INFORMATIONAL	found=[]	
active	**error_pages**	differential-probe	**COMPLETED**	INFORMATIONAL	tokens=[]	
active	**open_redirect**	param-probe	**COMPLETED**	INFORMATIONAL	param=None	
active	**host_header**	reflection-probe	**COMPLETED**	INFORMATIONAL	reflected=False	
active	**injection_indicators**	form-probe	**SKIPPED**	INFORMATIONAL	State-changing/non-GET form not submitted by default	POST probes require an explicitly authorized test mode
active	**injection_indicators**	form-probe	**SKIPPED**	INFORMATIONAL	State-changing/non-GET form not submitted by default	POST probes require an explicitly authorized test mode
active	**injection_indicators**	form-probe	**SKIPPED**	INFORMATIONAL	State-changing/non-GET form not submitted by default	POST probes require an explicitly authorized test mode
active	**injection_indicators**	form-probe	**SKIPPED**	INFORMATIONAL	State-changing/non-GET form not submitted by default	POST probes require an explicitly authorized test mode
active	**injection_indicators**	form-probe	**SKIPPED**	INFORMATIONAL	State-changing/non-GET form not submitted by default	POST probes require an explicitly authorized test mode
active	**injection_indicators**	form-probe	**SKIPPED**	INFORMATIONAL	State-changing/non-GET form not submitted by default	POST probes require an explicitly authorized test mode
active	**injection_indicators**	form-probe	**SKIPPED**	INFORMATIONAL	State-changing/non-GET form not submitted by default	POST probes require an explicitly authorized test mode
active	**injection_indicators**	form-probe	**SKIPPED**	INFORMATIONAL	State-changing/non-GET form not submitted by default	POST probes require an explicitly authorized test mode
active	**injection_indicators**	probe	**COMPLETED**	MEDIUM	params_tested=15 requests=56 timeouts=9	Benign indicator probes only; a finding here means 'investigate', not 'confirmed exploitable'
active	**ssrf_candidates**	param-name-match	**COMPLETED**	INFORMATIONAL	candidates=1	
active	**auth_session**	forms-and-errors	**COMPLETED**	INFORMATIONAL	forms_tested=0 issues=0 mfa_indicator=False	

سطح	ماژول	بررسی	وضعیت	اطمینان	مدرک	محدودیت
passive	**cpe_cve_correlation**	osv-live-enrichment	**COMPLETED**	INFORMATIONAL	candidates=1 osv_cves=0 osv_queries=0 osv_failures=0	Live CVE enrichment via OSV.dev for versioned CPE matches; offline NVD note retained as fallback for unversioned candidates.

16 فهرست نقاط پایانی، API و سطح حمله

ناسه ش	متد	نقطه پایانی	منبع
1	GET	[redacted]	discovery
2	GET	[redacted]	discovery
3	GET	[redacted]	discovery
4	GET	[redacted]	discovery
5	GET	[redacted]	discovery
6	GET	[redacted]	discovery
7	GET	[redacted]	discovery
8	GET	[redacted]%d9%85%d8%a7%d8%af/	discovery
9	GET	[redacted]	discovery
10	GET	[redacted]	discovery
11	GET	[redacted]	discovery
12	GET	[redacted]	discovery
13	GET	[redacted]	discovery
14	GET	[redacted]	discovery
15	GET	[redacted]D9%85-%D9%BE%D8%B1%D8%B3%D8%AA%D8%A7%D8%B1%DB%8C/	discovery
16	GET	[redacted]%D9%86%D9%87/%D8%A7%D8%B3%D9%84%DB%8C%D9%BE-%D9%86%DB%8C%D9%85-%D9%BE%D8%A7/	discovery
17	GET	[redacted]%D9%86%D9%87/%D8%B4%D9%88%D8%B1%D8%AA/	discovery
18	GET	[redacted]%D9%86%D9%87/couple-set/	discovery
19	GET	[redacted]	discovery
20	GET	[redacted]	discovery
21	GET	[redacted]%D8%AF%D8%A7%D9%85%D9%86-%D9%88-%D8%AF%D8%A7%D9%85%D9%86-%D8%B4%D9%88%D8%B1%D8%AA%DB%8C/	discovery
22	GET	[redacted]%D9%84%D8%A8%D8%A7%D8%B3-%D8%AE%D9%88%D8%A7%D8%A8-%DA%86%D8%B1%D9%85-%D9%88-%D9%84%D8%A7%D8%AA%DA%A9%D8%B3/	discovery
23	GET	[redacted]%DA%A9%D8%A7%D8%B3%D8%AA%D9%88%D9%85-%D8%AF%D8%A7%D9%86%D8%B4-%D8%A2%D9%85%D9%88%D8%B2%DB%8C/	discovery
24	GET	[redacted]%DA%A9%D8%A7%D8%B3%D8%AA%D9%88%D9%85-%D9%BE%D8%B1%D8%B3%D8%AA%D8%A7%D8%B1%DB%8C/	discovery
25	GET	[redacted]body-zanane/	discovery
26	GET	[redacted]%85-%D8%AE%D8%AF%D9%85%D8%AA%DA%A9%D8%A7%D8%B1%DB%8C/	discovery
27	GET	[redacted]kostom-lebas-raqs-arabi/	discovery
28	GET	[redacted]kostom-police-dozd-zanane/	discovery
29	GET	[redacted]lebas-khab-fantasy-zanane/	discovery
30	GET	[redacted]lebas-khab-rahaati-zanane/	discovery
31	GET	[redacted]db%8c/	discovery
32	GET	[redacted]	discovery
33	GET	[redacted]	discovery
34	GET	[redacted]%d9%86%d9%87/	discovery
35	GET	[redacted]%d9%86%d9%87/%d8%a7%d8%b3%d9%84%db%8c%d9%be-%d9%86%db%8c%d9%85-%d9%be%d8%a7/	discovery

ناسه ش	متد	نقطه پایانی	منبع
36	GET	%d9%86%d9%87/%d8%a7%d8%b3%d9%84%db%8c%d9%be-%d9%86%db%8c%d9%85-%d9%be%d8%a7/page/2/	discovery
37	GET	%d9%86%d9%87/%d8%b4%d9%88%d8%b1%d8%aa/	discovery
38	GET	%d9%86%d9%87/%d8%b4%d9%88%d8%b1%d8%aa/page/2/	discovery
39	GET	%d9%86%d9%87/%da%a9%d8%a7%d8%b3%d8%aa%d9%88%d9%85-%d9%88-%d9%84%d8%a8%d8%a7%d8%b3%d8%ae%d9%88%d8%a7%d8%a8/	discovery
40	GET	%d9%86%d9%87/couple-set/	discovery
41	GET	%d9%86%d9%87/couple-set/page/2/	discovery
42	GET		discovery
43	GET		discovery
44	GET	%d8%af%d8%a7%d9%85%d9%86-%d9%88-%d8%af%d8%a7%d9%85%d9%86-%d8%b4%d9%88%d8%b1%d8%aa%db%8c/	discovery
45	GET	%d8%af%d8%a7%d9%85%d9%86-%d9%88-%d8%af%d8%a7%d9%85%d9%86-%d8%b4%d9%88%d8%b1%d8%aa%db%8c/page/2/	discovery
46	GET	%d9%84%d8%a8%d8%a7%d8%b3-%d8%ae%d9%88%d8%a7%d8%a8-%da%86%d8%b1%d9%85-%d9%88-%d9%84%d8%a7%d8%aa%da%a9%d8%b3/	discovery
47	GET	%d9%84%d8%a8%d8%a7%d8%b3-%d8%ae%d9%88%d8%a7%d8%a8-%da%86%d8%b1%d9%85-%d9%88-%d9%84%d8%a7%d8%aa%da%a9%d8%b3/page/2/	discovery
48	GET	%da%a9%d8%a7%d8%b3%d8%aa%d9%88%d9%85-%d8%af%d8%a7%d9%86%d8%b4-%d8%a2%d9%85%d9%88%d8%b2%db%8c/	discovery
49	GET	%da%a9%d8%a7%d8%b3%d8%aa%d9%88%d9%85-%d8%af%d8%a7%d9%86%d8%b4-%d8%a2%d9%85%d9%88%d8%b2%db%8c/page/2/	discovery
50	GET	%da%a9%d8%a7%d8%b3%d8%aa%d9%88%d9%85-%d9%be%d8%b1%d8%b3%d8%aa%d8%a7%d8%b1%db%8c/	discovery
51	GET	%da%a9%d8%a7%d8%b3%d8%aa%d9%88%d9%85-%d9%be%d8%b1%d8%b3%d8%aa%d8%a7%d8%b1%db%8c/page/2/	discovery
52	GET	body-zanane/	discovery
53	GET	body-zanane/page/2/	discovery
54	GET	%85-%d8%ae%d8%af%d9%85%d8%aa%da%a9%d8%a7%d8%b1%db%8c/	discovery
55	GET	%85-%d8%ae%d8%af%d9%85%d8%aa%da%a9%d8%a7%d8%b1%db%8c/page/2/	discovery
56	GET	kostom-khedmatkari-pishkhedmat/	discovery
57	GET	kostom-lebas-raqs-arabi/	discovery
58	GET	kostom-police-dozd-zanane/	discovery
59	GET	lebas-khab-fantasy-zanane/	discovery
60	GET	lebas-khab-fantasy-zanane/page/2/	discovery

نمایش 60 مورد از 400 نقطه پایانی. فهرست کامل در خروجی JSON موجود است.

17 تفاوت اسکن و ردیابی ارزیابی

جدید	رفع‌شده	بدون تغییر
0	0	15
از اسکن قبلی این مجموعه	از اسکن قبلی این مجموعه	از اسکن قبلی این مجموعه حفظ‌شده

اثرانگشت‌های جدید: هیچ‌کدام

18 روش‌شناسی، مرز ایمنی و تفسیر

تفسیر
غیرفعال ایمن: DNS، TLS و گواهی، هدرهای امنیتی HTTP، وضعیت احراز هویت ایمیل، شناسایی غیرفعال، غنی‌سازی از طریق شفافیت گواهی، غنی‌سازی زنده‌ی CVE از طریق OSV.dev (در صورت شناسایی به‌عنوان جایگزین CVE نسخه‌دار)، و همبستگی آفلاین نرم‌افزار/یادداشت CPE.
کامل (غیرفعال ایمن + فعال): بررسی‌های محدود مواجهه‌ی TCP، خزش هم‌مبدا، شناسایی API و OpenAPI، بازتاب بی‌خطر، بررسی‌های CORS و هدر Host، بررسی‌های خطا و متد، و نشانه‌های غیرمخرب تزریق، احراز هویت و نامزدهای SSRF.
خارج از محدوده: حمله‌ی credential stuffing، brute force، ماندگاری (persistence)، بارهای مخرب، بارگذاری فایل، اقدامات وضعیت‌تغییردهنده در برنامه، اجرای سوءاستفاده (exploit)، و callback یا fetch های SSRF.
نتیجه‌ی «قبول» به این معناست که بررسی موردنظر بدون یافته‌ای تکمیل شده است. این امر عدم وجود آسیب‌پذیری خارج از محدوده‌ی پوشش‌داده‌شده را اثبات نمی‌کند.
برچسب‌های OWASP، WSTG و ASVS نگاشت‌های زمینه‌ای هستند، نه یک گواهی یا تاییدیه‌ی رسمی انطباق. مقادیر CVE تنها در صورت وجود در مدرک نمایش داده می‌شوند.
ماژول‌های ردشده، ناموفق و پایان‌مهلت‌یافته در بخش 15 فهرست شده‌اند، تا «یافت نشد» هرگز با «تست نشد» اشتباه گرفته نشود.

مدل امتیازدهی
CVSS و شدت: هر امتیاز پایه از روی بردار CVSS 3.1 و با استفاده از فرمول رسمی FIRST 4.0 چاپ‌شده در بخش 13، کم زیر 4.0+، متوسط 7.0+، زیاد 9.0+، بحرانی (محاسبه می‌شود. شدت، باند استاندارد است. تاثیر را در صورت واقعی‌بودن ضعف بیان می‌کند؛ میزان اعتبارسنجی ابزار را در بر نمی‌گیرد.
اولویت P0 تا P4 (فوریت): CVSS × 10 وزن‌دهی‌شده بر اساس اطمینان، وضعیت تاییدیه، میزان مدرک، مواجهه‌ی دارایی و دسته‌بندی. از این رو یک نشانه‌ی تاییدنشده رتبه‌ای پایین‌تر از یک واقعیت تاییدشده یا مستقیما مشاهده‌شده با CVSS برابر می‌گیرد. باندها: P0 به‌بالای 90، P1 به‌بالای 75، P2 به‌بالای 55، P3 به‌بالای 30، در غیر این صورت P4.
امتیاز امنیتی (0 تا 100، بالاتر بهتر است؛ مدل امتیازدهی 2): 100 منهای کسر وزن‌دهی‌شده‌ی سه ریسک دسته‌ای (زیرساخت 35٪، نشت داده 35٪، سمت کلاینت 30٪)، ترکیب‌شده با نسبت 75/25 با یک عبارت ریسک کلی. در هر دسته و در مجموع، بدترین یافته به‌طور کامل و هر یافته‌ی بعدی با نیمی از وزن محاسبه می‌شود، بنابراین تعداد زیادی نقص جزئی نمی‌تواند بر یک مواجهه‌ی بحرانی تاییدشده غلبه کند و هیچ یافته‌ی اضافه‌ای امتیاز را افزایش نمی‌دهد.
گزارشی بدون هیچ یافته‌ای در سقف 90 محدود می‌شود: نبود یافته، اثبات نبود ریسک نیست. این امتیاز یک شاخص تقریبی برای پیگیری تغییر در طول زمان است، نه یک گواهی، و تنها با امتیازهای پیشین تولیدشده توسط همین مدل امتیازدهی مقایسه می‌شود.