SaliSecure

شناسه اسکن
https://salisec.ir

IP
/ مدت زمان 428.3 ثانیه

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.

مواجهه بالا
وضعیت کلی امنیت

امتیاز، شاخصی وزنی بر اساس ضعف‌های مشاهده‌شده و بررسی‌های انجام‌شده است؛ یک گواهی رسمی نیست.

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 ارزیابی کنترل‌ها

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 اقدامات اولویت‌دار

#	ریسک	چرا اهمیت دارد	چه اتفاقی می‌تواند بیفتد	اقدام	میزان تلاش
1	بحرانی / P2	رفتار پاسخ نشان می‌دهد که پارامتر ممکن است بدون پاکسازی 'cat' مناسب، روی یک کوئری/قالب SSTI در یک‌اند تاثیر بگذارد	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.	ابتدا اعتبارسنجی دستی 1 نشانه و سپس رفع آن‌ها: از کوئری‌های پارامتری‌شده / یک template engine با استفاده کنید؛ تمام ورودی کاربر را auto-escaping سمت سرور اعتبارسنجی و encode کنید	متوسط
2	زیاد / P2	رفتار پاسخ نشان می‌دهد که پارامتر ممکن است بدون پاکسازی 'cat' مناسب، روی یک کوئری/قالب در یک‌اند تاثیر بگذارد NoSQLi	در صورت تایید، مهاجم می‌تواند به داده‌های مهم دسترسی پیدا کند یا آن‌ها را تغییر دهد، یا بخش‌هایی از سایت را مختل کند.	ابتدا اعتبارسنجی دستی 1 نشانه و سپس رفع آن‌ها: از کوئری‌های پارامتری‌شده / یک template engine با استفاده کنید؛ تمام ورودی کاربر را auto-escaping سمت سرور اعتبارسنجی و encode کنید	متوسط
3	زیاد / P3	رفتار پاسخ نشان می‌دهد که پارامتر ممکن است بدون پاکسازی 'cat' مناسب، روی یک کوئری/قالب SQLi در یک‌اند تاثیر بگذارد	در صورت تایید، مهاجم می‌تواند به داده‌های مهم دسترسی پیدا کند یا آن‌ها را تغییر دهد، یا بخش‌هایی از سایت را مختل کند.	ابتدا اعتبارسنجی دستی 1 نشانه و سپس رفع آن‌ها: از کوئری‌های پارامتری‌شده / یک template engine با استفاده کنید؛ تمام ورودی کاربر را auto-escaping سمت سرور اعتبارسنجی و encode کنید	متوسط
4	متوسط / P3	امکان جعل ایمیل و فیشینگ با استفاده از دامنه‌ی هدف را فراهم می‌کند	حملات دیگر را آسان‌تر می‌کند یا می‌تواند برخی اطلاعات را افشا کند.	سیاست DMARC را روی p=quarantine یا p=reject تنظیم کنید	متوسط
5	زیاد / P3	رفتار پاسخ نشان می‌دهد که پارامتر ممکن است بدون پاکسازی 'cat' مناسب، روی یک کوئری/قالب LDAP در یک‌اند تاثیر بگذارد	در صورت تایید، مهاجم می‌تواند به داده‌های مهم دسترسی پیدا کند یا آن‌ها را تغییر دهد، یا بخش‌هایی از سایت را مختل کند.	ابتدا اعتبارسنجی دستی 1 نشانه و سپس رفع آن‌ها: از کوئری‌های پارامتری‌شده / یک template engine با استفاده کنید؛ تمام ورودی کاربر را auto-escaping سمت سرور اعتبارسنجی و encode کنید	متوسط

03 شاخص مواجهه با ریسک (تقریبی)



بررسی‌های تکمیل‌شده: 39 از 39. 0 مورد تکمیل‌نشده؛ حوزه‌های دارای برچسب «تست‌نشده» یا «بازبینی» سالم شمرده نمی‌شوند. مدرک سطح-دستور و پیوست کامل یافته‌ها در گزارش فنی، در همان پوشه، موجود است.

محدوده: ارزیابی مجاز، فقط‌خواندنی و غیرمخرب. هیچ سوءاستفاده‌ای انجام نشد. اسکن 2026/11/03 /