EXECUTIVE SECURITY SUMMARY / ONE PAGE

IP / 2026-11-03 / 12-MIN DEEP PROFESSIONAL / Safe Passive + Active
Scan ID / Duration 428.3 s
https://salisec.ir

OVERALL POSTURE

HIGH EXPOSURE

9 confirmed or observed weakness(es) and 6 unverified indicator(s) identified. The score includes unverified indicators and will change after manual validation.

The score is a weighted index of observed weaknesses and completed checks. It is not a certification.

SECURITY SCORE	WEAKNESSES	CONFIRMED / OBSERVED	CHECKS COMPLETED	TREND VS PREVIOUS
49 /100	15	9	100%	+0
High exposure	Critical 1 / High 3 / Medium 8 / Low 3	6 unverified indicator(s) to validate	39 of 39 modules, 0 not completed	vs 49/100 on 2026-11-01 (same test set)

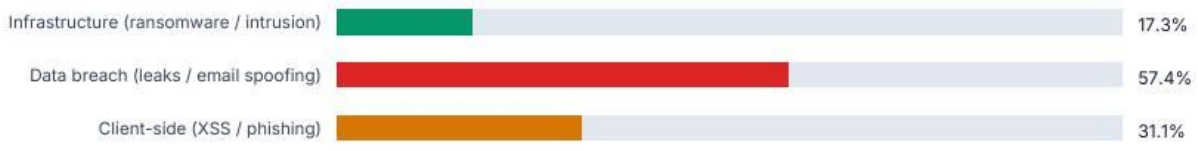
01 CONTROL ASSESSMENT

CONTROL AREA	STATUS	FINDING SUMMARY	EVIDENCE BASIS
Transport and TLS	PASS	Modern TLS only, certificate valid for 165 days	TLSv1.3 / TLS_AES_256_GCM_SHA384
Email authentication	RISK	No DMARC enforcement: the domain can be spoofed	SPF: VALID
Web security headers	RISK	5 of 6 observed security headers missing	Missing: HSTS, CSP, X-Frame, X-Content, Referrer
Exposed network services	PASS	No reachable services among 9 probed ports	Bounded TCP probe of predefined common ports
Input handling (injection)	VERIFY	4 indicator(s) need manual verification	Module did not complete (completed/skipped); results are not conclusive
Attack-surface discovery	INFO	400 endpoints / 8 subdomains / 115 forms	100 pages crawled / 2 JS files / 0 API spec(s)

02 PRIORITY ACTIONS

#	RISK	WHY IT MATTERS	WHAT COULD HAPPEN	ACTION	EFFORT
1	P2 / Critical	Response behaviour suggests the 'cat' parameter may influence a backend SSTI query/template without proper sanitisation	If confirmed, an attacker could run their own commands on your web server, in the worst case taking over the whole website and everything stored on it.	Validate 1 indicator(s) manually, then remediate: Use parameterised queries / an auto-escaping template engine; validate and encode all user input server-side	Medium
2	P2 / High	Response behaviour suggests the 'cat' parameter may influence a backend NoSQLi query/template without proper sanitisation	If confirmed, an attacker could read or change data in your database without logging in, by sending specially crafted values.	Validate 1 indicator(s) manually, then remediate: Use parameterised queries / an auto-escaping template engine; validate and encode all user input server-side	Medium
3	P3 / High	Response behaviour suggests the 'cat' parameter may influence a backend SQLi query/template without proper sanitisation	If confirmed, an attacker could read, change or delete data in your database, such as customers, orders and admin passwords, just by typing crafted text into a form field or web address.	Validate 1 indicator(s) manually, then remediate: Use parameterised queries / an auto-escaping template engine; validate and encode all user input server-side	Medium
4	P3 / Medium	Allows email spoofing and phishing using target domain	Anyone could send emails that look like they come from your domain, such as fake invoices or password-reset mails to your customers and staff.	Set DMARC policy to p=quarantine or p=reject	Medium
5	P3 / High	Response behaviour suggests the 'cat' parameter may influence a backend LDAP query/template without proper sanitisation	If confirmed, an attacker could get around login checks or read your staff and user directory.	Validate 1 indicator(s) manually, then remediate: Use parameterised queries / an auto-escaping template engine; validate and encode all user input server-side	Medium

03 RISK EXPOSURE INDEX (HEURISTIC)



Checks completed: 39 of 39. 0 not completed; areas marked NOT TESTED or REVIEW are not counted as clean. Command-level evidence and the complete findings appendix are in the Technical Report in the same folder.

Scope: authorized, read-only, non-destructive assessment. No exploitation was attempted. Scan / 2026-11-03.