MANGUDAİ

"We scout your attack surface before attackers do."

Target Host: enterprise-target.com

Start Time: 2026-07-13 10:46

Finish Time: 2026-07-13 11:46

Security Score: **58/100**

Executive Summary

Mangudai scouted this target's digital footprint. Below is the automated analysis of vulnerabilities, SSL configuration, DNS settings, exposed files, and port statuses.

Mangudai AI Analysis

Mangudai has completed a non-intrusive outer perimeter security assessment of enterprise-target.com. The security posture is currently evaluated at a score of 58/100, indicating moderate exposure. The automated discovery identified 14 active subdomains, 3 exposed services, and several configuration vulnerabilities. The most critical exposure is the presence of 4 employee email accounts with leaked credentials on the dark web, posing an immediate risk of credential stuffing and corporate identity theft. Additionally, the domain lacks an active DMARC record, and one of the subdomains hosts an outdated Apache server vulnerable to remote information disclosure.

Vulnerability Findings

Vulnerability Title	Severity	CVSS Score	Confidence
Employee Credentials Leaked on Dark Web	CRITICAL	9.3	100%
Missing DMARC DNS Record	HIGH	7.5	100%
Outdated Web Server Version Detected	MEDIUM	6.2	100%
Insecure SSL/TLS Cipher Suites Enabled	LOW	3.8	100%

Detailed Vulnerability Report

1. [CRITICAL] Employee Credentials Leaked on Dark Web

Affected Hosts (1): mail.enterprise-target.com

Description: Multiple corporate email accounts were found in recent third-party data breaches on the dark web. The leaks contain plaintext or weak hashes of employee passwords.

Remediation:

Enforce multi-factor authentication (MFA) immediately across all corporate portals and require affected employees to reset their passwords.

2. [HIGH] Missing DMARC DNS Record

Affected Hosts (1): enterprise-target.com

Description: No DMARC record was found on the domain. This allows malicious actors to send unauthorized emails spoofing your company's domain name.

Remediation:

Publish a valid DMARC TXT record under _dmarc.enterprise-target.com with a policy of 'p=quarantine' or 'p=reject'.

3. [MEDIUM] Outdated Web Server Version Detected

Affected Hosts (1): dev.enterprise-target.com

Description: An outdated Apache 2.4.41 web server was detected on dev.enterprise-target.com, which is known to be vulnerable to multiple CVEs.

Remediation:

Update the web server instance to the latest stable version of Apache or migrate behind a proxy.

4. [LOW] Insecure SSL/TLS Cipher Suites Enabled

Affected Hosts (1): mail.enterprise-target.com

Description: The SSL/TLS configuration on mail.enterprise-target.com allows the use of deprecated TLS 1.0 and TLS 1.1 protocols.

Remediation:

Disable TLS 1.0 and 1.1 protocols, and enforce the use of TLS 1.2 and TLS 1.3 with secure cipher suites.

Discovered Assets

Type	Value
IP ADDRESS	104.26.15.22
IP ADDRESS	172.67.74.19
PORT	25 (SMTP)
PORT	443 (HTTPS)
PORT	80 (HTTP)
SUBDOMAIN	api.enterprise-target.com
SUBDOMAIN	dev.enterprise-target.com
SUBDOMAIN	mail.enterprise-target.com
SUBDOMAIN	www.enterprise-target.com