

# Executive Summary Report

Acunetix Security Audit

2025-04-29

# Scan of simpan.pu.go.id

## Scan details

Scan information	
Start time	2025-04-29T00:32:09.280124+07:00
Start url	<a href="https://simpan.pu.go.id/seleksi-pengurus-x/">https://simpan.pu.go.id/seleksi-pengurus-x/</a>
Host	simpan.pu.go.id
Scan time	37 minutes, 17 seconds
Profile	Full Scan
Server information	Apache/2.4.58 (Ubuntu)
Responsive	True
Server OS	Unix

## Threat level

### Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

## Alerts distribution

Total alerts found	27
❗ High	1
⚠️ Medium	5
❕ Low	8
ⓘ Informational	13

## Executive summary

Alert group	Severity	Alert count
Cross site scripting	High	1
Development configuration files	Medium	1
Password field submitted using GET method	Medium	1
TLS 1.0 enabled	Medium	1
TLS/SSL Sweet32 attack	Medium	1
TLS/SSL Weak Cipher Suites	Medium	1
Clickjacking: X-Frame-Options header missing	Low	1
Cookies without Secure flag set	Low	1
Documentation files	Low	1
File uploads	Low	1
HTTP Strict Transport Security (HSTS) not implemented	Low	1
Insecure Inline Frame (iframe)	Low	1
Login page password-guessing attack	Low	1
Session token in URL	Low	1