Executive Summary Report

Acunetix Security Audit

17 January 2019

Generated by Acunetix

Vulnerabilities

Scan details

Scan information	
Start url	http://192.168.1.62/rae3d_2/
Host	http://192.168.1.62/

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	251
High	84
Medium	52
Low	11
Informational	104

Executive summary

Alert group	Severity	Alert count
Cross site scripting	High	84
Directory listing	Medium	44
User credentials are sent in clear text	Medium	2
Vulnerable Javascript library	Medium	2
Application error message	Medium	1
Backup files	Medium	1
Host header attack	Medium	1
HTML form without CSRF protection	Medium	1
Documentation file	Low	6
Clickjacking: X-Frame-Options header missing	Low	1
Cookie(s) without HttpOnly flag set	Low	1
Cookie(s) without Secure flag set	Low	1
Login page password-guessing attack	Low	1
TRACE method is enabled	Low	1

Vulnerabilities

Scan details

Scan information	
Start url	http://localhost:1234/projects/Atmrs/
Host	http://localhost:1234/

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	157
High	84
Medium	50
Low	16
Informational	7

Executive summary

Alert group	Severity	Alert count
Cross site scripting	High	84
Directory listing	Medium	39
User credentials are sent in clear text	Medium	2
Vulnerable Javascript library	Medium	2
Apache server-info enabled	Medium	1
Apache server-status enabled	Medium	1
Application error message	Medium	1
Backup files	Medium	1
Host header attack	Medium	1
HTML form without CSRF protection	Medium	1
Test CGI script leaking environment variables	Medium	1
Documentation file	Low	11
Clickjacking: X-Frame-Options header missing	Low	1
Cookie(s) without HttpOnly flag set	Low	1
Cookie(s) without Secure flag set	Low	1
Login page password-guessing attack	Low	1
TRACE method is enabled	Low	1