



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.

Scan Detail

Target	http://rest.vulnweb.com/
Scan Type	Full Scan
Start Time	Jul 26, 2022, 3:39:25 PM GMT
Scan Duration	1 hour, 25 minutes
Requests	74216
Average Response Time	162ms
Maximum Response Time	1407ms



High



Medium



Low



Informational

Severity

Vulnerabilities

Instances

High	3	76
Medium	3	4
Low	1	1
Informational	5	6
Total	12	87

Informational



	Instances
Content Security Policy (CSP) not implemented	1
Content type is not specified	1
No HTTP Redirection	1
Others	3

Low Severity



	Instances
Clickjacking: X-Frame-Options header	1

Medium Severity



	Instances
Basic authentication over HTTP	1
Unencrypted connection	1
Vulnerable JavaScript libraries	2

High Severity



	Instances
Weak password	1
XML external entity injection	25
XML external entity injection via external file	50

Impacts

Severity Filter: High Medium Low Informational

SEVERITY	IMPACT
High	1 Weak password
High	25 XML external entity injection
High	50 XML external entity injection via external file
Medium	1 Basic authentication over HTTP
Medium	1 Unencrypted connection
Medium	2 Vulnerable JavaScript libraries
Low	1 Clickjacking: X-Frame-Options header
Informational	1 Content Security Policy (CSP) not implemented
Informational	1 Content type is not specified
Informational	1 No HTTP Redirection
Informational	2 Outdated JavaScript libraries
Informational	1 PHP Version Disclosure