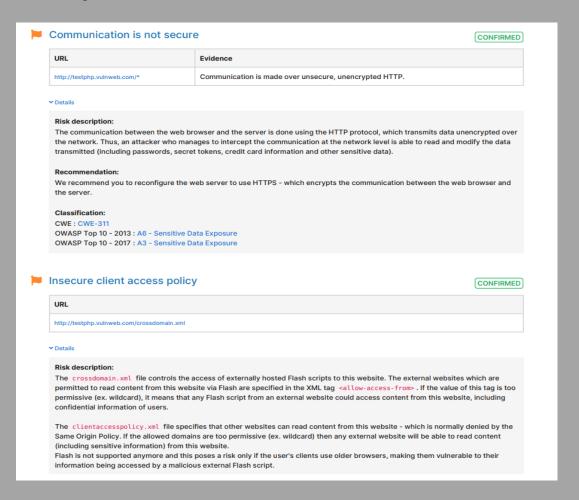
Vulnerability report for " http://testphp.vulnweb.com/* "

Summary

It is Observed that website assessed it is observed that site is Insecure as the communication between the web browser and the server is done using the HTTP protocol, which transmits data unencrypted over the network. Thus, an attacker who manages to intercept the communication at the network level is able to read and modify the data transmitted (including passwords, secret tokens, credit card information and other sensitive data). There are also other vulnerabilities found from the quick assessment done with the help of Pentest tool which is a powerfull website scanner

Findings



Server software and technology found

UNCONFIRMED 6

Software / Version	Category
Nginx 1.19.0	Web servers, Reverse proxies

✓ Details

Risk description:

An attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:

We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

References

 $https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server.html$

Classification:

OWASP Top 10 - 2013: A5 - Security Misconfiguration OWASP Top 10 - 2017: A6 - Security Misconfiguration

Security.txt file is missing

CONFIRMED

URI

Missing: http://testphp.vulnweb.com/.well-known/security.txt

✓ Detail:

Risk description

We have detected that the server is missing the security.txt file. There is no particular risk in not creating a valid Security.txt file for your server. However, this file is important because it offers a designated channel for reporting vulnerabilities and security issues.

Recommendation

We recommend you to implement the security.txt file according to the standard, in order to allow researchers or users report any security issues they find, improving the defensive mechanisms of your server.

References

https://securitytxt.org/

Classification:

OWASP Top 10 - 2013: A5 - Security Misconfiguration OWASP Top 10 - 2017: A6 - Security Misconfiguration

Scan Information

Scan information:

• Start time: Nov 16, 2023 / 18:09:49

• Finish time: Nov 16, 2023 / 18:10:04

• Scan duration: 15 sec

• Scan Type: Lite Scan

• Done by : OPENCS - Tests performed: 19/19