Client

Name	Contact
Qatar Company - IT	00998877

Document Control

Author	Testers	Reviewers
Faher	Faher Bakri	None

Start Date	2020-08-06
End Date	2020-08-13
Last Modified	
Version	

Executive Summary

1

Vulnerabilities

Name	Severity	Status
Stored XSS	critical	open
Reflected XSS	high	open
Server Version Disclosure	info	open

Severity of Vulnerabilities

Severity	Number of Vulnerabilities
Critical	1
High	1
Medium	0
Low	0
Info	1

Scope

1

Target

Infrastructure

Description

best description
new line

Vulnerability #1 - Stored XSS

Summary

Name	Stored XSS
Severity	critical
Status	open
Exploitability	hacker
OWASP Top 10 Mapping	Cross-Site Scripting XSS

Risk/Impact

Stealing customer cookies

Description

Cross-site Scripting (XSS) is a client-side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application.

POC

<script>alert(1)</script>

Remidiation

To keep yourself safe from XSS, you must sanitize your input. Your application code should never output data received as input directly to the browser without checking it for malicious code.

Comments

None

References

https://www.acunetix.com/websitesecurity/cross-site-scripting/

Vulnerability #2 - Reflected XSS

Summary

Name	Reflected XSS
Severity	high
Status	open
Exploitability	hacker
OWASP Top 10 Mapping	Cross-Site Scripting XSS

Risk/Impact

Stealing customer cookies

Description

Cross-site Scripting (XSS) is a client-side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application.

POC

<script>alert(1)</script>

Remidiation

To keep yourself safe from XSS, you must sanitize your input. Your application code should never output data received as input directly to the browser without checking it for malicious code.

Comments

None

References

https://www.acunetix.com/websitesecurity/cross-site-scripting/

Vulnerability #3 - Server Version Disclosure

Summary

Name	Server Version Disclosure
Severity	info
Status	open
Exploitability	hacker
OWASP Top 10 Mapping	Security Misconfiguration

Risk/Impact

data about used technologies

Description

Server replies with

POC

HTTP/1.1 200 OK Date: Thu, 12 Jun 2014 14:15:01 GMT Server: Apache/2.2.21 (Win32) PHP/5.4.7 Content-Length:226 Connection: close Content-Type: text/html; charset=iso-8859-1

Remidiation

remove data from server response headers

Comments

None

References

https://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/