Qatar Company Pentest 2020 Summer - Report

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
SQL Injection	critical	Choose...
Vuln With POC	critical	open
Reflected XSS	high	open

Severity of Vulnerabilities

Severity	Number of Vulnerabilities
Critical	3
High	1
Medium	0
Low	0
Info	0

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 - SQL Injection

Summary

Name	SQL Injection
Severity	critical
Status	Choose...
Exploitability	Choose...
OWASP Top 10 Mapping	Injection

Risk/Impact

Description

POC

Remidiation

Comments

References

Vulnerability #3 - Vuln With POC

Summary

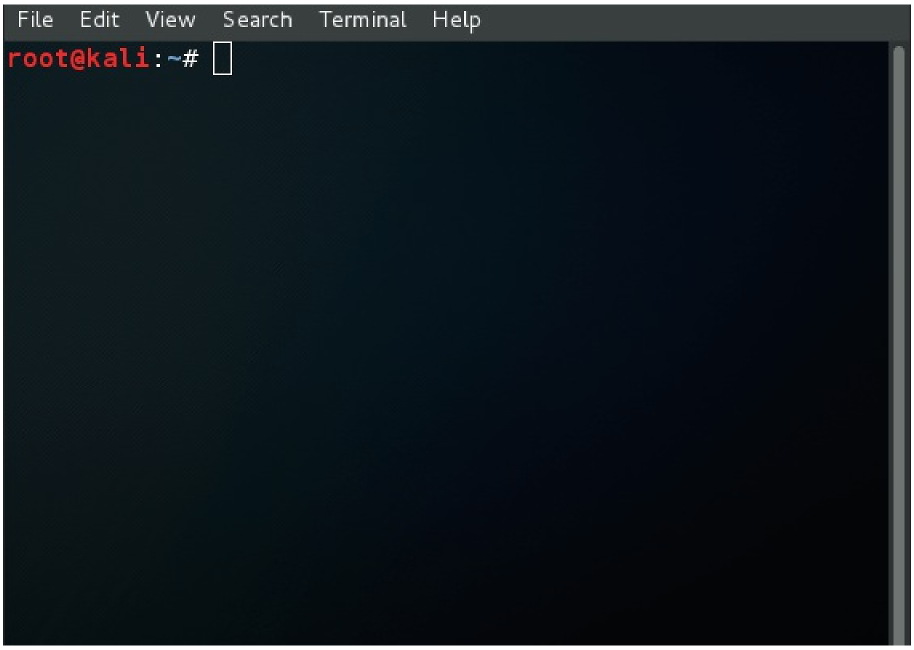
Name	Vuln With POC
Severity	critical
Status	open
Exploitability	hacker
OWASP Top 10 Mapping	Choose...

Risk/Impact

Description

POC

> sudo



```
root@kali:~# 
```

Remidiation

Comments

References

Vulnerability #4 - 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/