SecureCodingLab_18BCN7040_Shreejay

Vulnerability Report

Thursday, June 10, 2021

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	06/10/2021	A.Shreejay	Initial Version

Table of Contents

General Information

Scope

VIT-AP has mandated us to perform security tests on the following scope:

- External Pentest on VIT-AP Network

Organisation

The testing activities were performed between 06/07/2021 and 06/09/2021.

Executive Summary

VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
High	IDX-007	DOM XSS	API,DB,EXTERNAL THIRD PARTY AD
Medium	VULN-001	Security MisConfiguaration	
Medium	VULN-005	ClickJack	
Medium	VULN-003	ICS	
Medium	VULN-002	IDOR	

Technical Details

DOM XSS

CVSS Severity	**High**	**CVSSv3 Score**		**8.5**
CVSSv3 criterias	Attack Vector :	**Network**	Scope :	**Changed**
	Attack Complexity :	**High**	Confidentiality :	**High**
	Required Privileges :	**Low**	Integrity :	**High**
	User Interaction :	**None**	Availability :	**High**
Affected scope	API,DB,EXTERNAL THIRD PARTY AD			
Description	Asset Cloud			
Observation	Compromise in External API			
Test details				
Remediation	Periodical Checking in API Index Change Passwords			
References				

Security MisConfiguaration

CVSS Severity	**Medium**	**CVSSv3 Score**		**6.4**
CVSSv3 criterias	Attack Vector :	**Network**	Scope :	**Unchanged**
	Attack Complexity :	**Low**	Confidentiality :	**Low**
	Required Privileges :	**High**	Integrity :	**High**
	User Interaction :	**Required**	Availability :	**High**
Affected scope				
Description	Must be defined and deployed for the application,frameworks,database server			
Observation				
Test details				
Remediation				
References				

ClickJack

CVSS Severity	**Medium**	**CVSSv3 Score**		**6.3**
CVSSv3 criterias	Attack Vector :	**Network**	Scope :	**Unchanged**
	Attack Complexity :	**Low**	Confidentiality :	**Low**
	Required Privileges :	**Low**	Integrity :	**Low**
	User Interaction :	**None**	Availability :	**Low**
Affected scope				
Description	ClickJacking is a malicious technique of tricking a user into clicking on something from what the user perceives the potentially revealing confidential information or allowing others to take control of their computer while client seemingly innocuous objects,including web pages.As clickjack takes the form of embedded code of a script that can execute without the users knowledge.such as clicking on a button that appears to perform another function.			
Observation	Open any url that you want to test lets say https://www.incypts.com/ now just put <html>			
Test details				
Remediation	Use "X-FRAME" Options			
References				

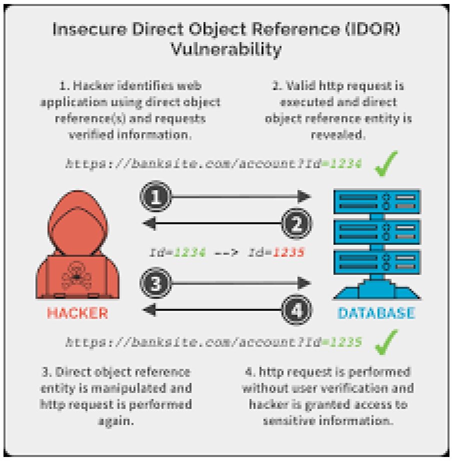
ICS

CVSS Severity	**Medium**	**CVSSv3 Score**		**5.9**
CVSSv3 criterias	Attack Vector :	**Network**	Scope :	**Unchanged**
	Attack Complexity :	**High**	Confidentiality :	**Low**
	Required Privileges :	**Low**	Integrity :	**None**
	User Interaction :	**None**	Availability :	**High**
Affected scope				
Description	Insecure Cryptographic Storage			
Observation	It is a common vulnerability which exists when the sensitive data is not stored securely			
Test details				
Remediation				
References				

IDOR

CVSS Severity	**Medium**	**CVSSv3 Score**		**4.2**
CVSSv3 criterias	Attack Vector :	**Network**	Scope :	**Unchanged**
	Attack Complexity :	**High**	Confidentiality :	**Low**
	Required Privileges :	**None**	Integrity :	**None**
	User Interaction :	**Required**	Availability :	**Low**
Affected scope				
Description	IDOR are a type of access control vulnerability			
Observation				

Test details



Insecure Direct Object Reference (IDOR) Vulnerability
1. Hacker identifies web application using direct object reference(s) and requests verified information.
2. Valid http request is executed and direct object reference entity is revealed.
https://banksite.com/account?Id=1234
1
2
Id=1234 --> Id=1235
3
4
HACKER
DATABASE
https://banksite.com/account?Id=1235
3. Direct object reference entity is manipulated and http request is performed again.
4. http request is performed without user verification and hacker is granted access to sensitive information.

Image 1 – IDOR.png

Remediation	
References	

ITLP

CVSS Severity	**None**	**CVSSv3 Score**	
CVSSv3 criterias	Attack Vector : Attack Complexity : Required Privileges : User Interaction :	Scope : Confidentiality : Integrity : Availability :	
Affected scope			
Description	Insufficient Transport Layer Protection		
Observation	Deals with information exchange between the user and the server		
Test details			
Remediation			
References			

XSS

CVSS Severity	**None**	**CVSSv3 Score**	
CVSSv3 criterias	Attack Vector : Attack Complexity : Required Privileges : User Interaction :	Scope : Confidentiality : Integrity : Availability :	
Affected scope			
Description	XSS is an attack which allows the attacker to execute scripts on the victims browser.		
Observation			
Test details			
Remediation			
References			