

SecureCodingLab\_19BCE7061\_Vakuladevi

# VULNERABILITY REPORT

THURSDAY, JUNE 10, 2021

---

**MODIFICATIONS HISTORY**

Version	Date	Author	Description
1.0	06/10/2021	Dollu Vakuladevi	Initial Version

---

TABLE OF CONTENTS

1. General Information ..... 4

1.1 Scope ..... 4

1.2 Organisation ..... 4

2. Executive Summary ..... 5

3. Technical Details ..... 6

3.1 title ..... 13

4. Vulnerabilities summary ..... 6

---

## GENERAL INFORMATION

---

### SCOPE

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

- External Pentest on VIT-APNetwork
- 

### 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 MisConfiguration	
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 :  Attack Complexity :  Required Privileges :  User Interaction :	Network  High  Low  None	Scope :  Confidentiality :  Integrity :  Availability :
	Changed  High  High  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 MISCONFIGURATION

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 depoloyed for the application,frameworks,database server			
OBSERVATION				
TEST DETAILS				
REMEDIATION				
REFERENCES				



## CLICKJACK

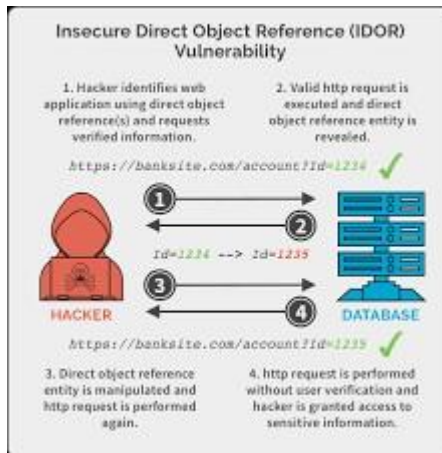
CVSS SEVERITY	Medium	CVSSv3 SCORE	6.3
CVSSv3 CRITERIAS	Attack Vector :  Attack Complexity :  Required Privileges :  User Interaction :	Network  Low  Low  None	Scope :  Confidentiality :  Integrity :  Availability :
AFFECTED SCOPE			
DESCRIPTION	ClickJacking is a malicious tecqnique of tricking a user 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 innocous objects,including web pages.As clickjack takes the form of embedded code of a script that can executewithout the users knowledge.suchn 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 : <b>Network</b> Scope : <b>Unchanged</b> Attack Complexity : <b>High</b> Confidentiality : <b>Low</b> Required Privileges : <b>None</b> Integrity : <b>None</b> User Interaction : <b>Required</b> Availability : <b>Low</b>		
AFFECTED SCOPE			
DESCRIPTION	IDOR are a type of access control vulnerability		
OBSERVATION			
TEST DETAILS	 <p><b>Insecure Direct Object Reference (IDOR) Vulnerability</b></p> <p>1. Hacker identifies web application using direct object reference(s) and requests verified information.</p> <p>2. Valid http request is executed and direct object reference entity is revealed.</p> <p><code>https://banksite.com/account?id=1234</code> ✓</p> <p>3. Direct object reference entity is manipulated and http request is performed again.</p> <p>4. http request is performed without user verification and hacker is granted access to sensitive information.</p> <p><code>https://banksite.com/account?id=1235</code> ✓</p> <p>Image 1 – IDOR.png</p>		
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			

