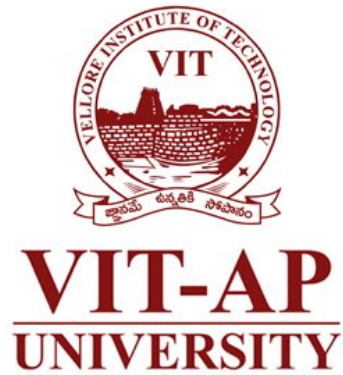


Vit-Ap External Audit

VULNERABILITY REPORT

MONDAY, MAY 31, 2021



MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	05/31/2021	DEVI JAGANNADH 2	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.....	6
4.	Vulnerabilities summary.....	8

GENERAL INFORMATION

SCOPE

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

- All the nodes in infra.

ORGANISATION

The testing activities were performed between 05/17/2021 and 05/31/2021.

EXECUTIVE SUMMARY

VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

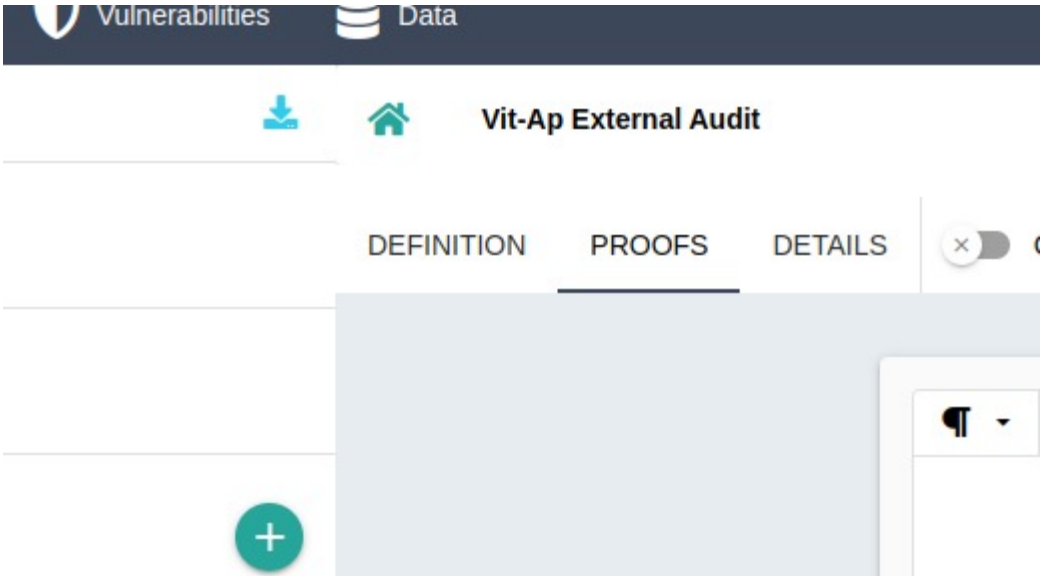
Risk	ID	Vulnerability	Affected Scope
High	IDX-002	DOM XSS	
High	IDX-003	CSRF	
Medium	VULN-001	Clickjacking	

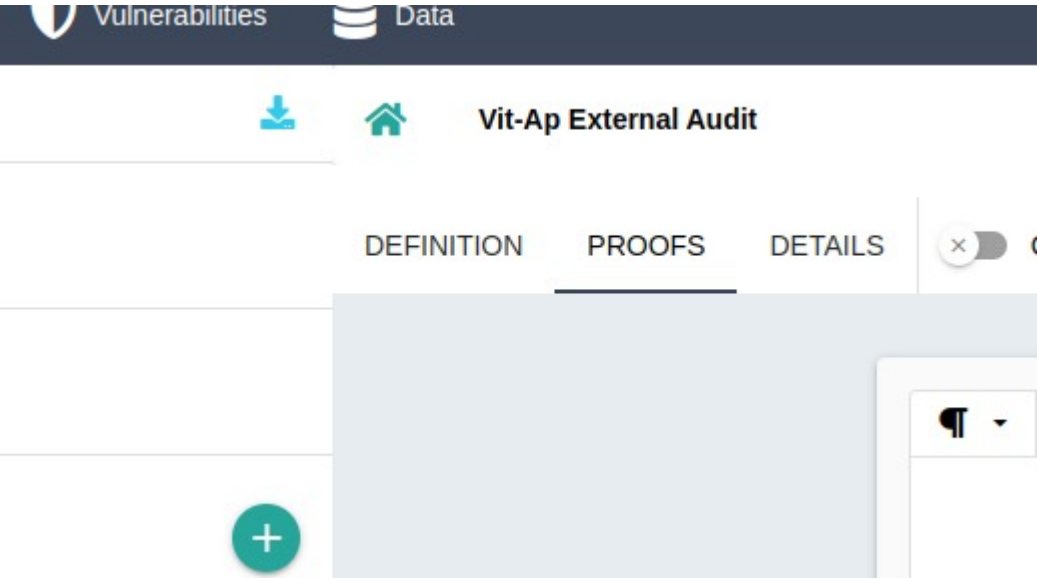
TECHNICAL DETAILS

DOM XSS

CVSS SEVERITY	High	CVSSv3 SCORE	7.6
CVSSv3 CRITERIAS	Attack Vector : Network Attack Complexity : Low Required Privileges : Low User Interaction : Required	Scope : Changed Confidentiality : High Integrity : Low Availability : None	
AFFECTED SCOPE			
DESCRIPTION	DOM XSS stands for Document Object Model-based Cross-site Scripting All HTML documents have an associated DOM that consists of objects, which represent document properties from the point of view of the browser. When a client-side script is executed, it can use the DOM of the HTML page where the script runs.		
OBSERVATION	1)Open any url which you want to test let's say https://www.incrypts.com/ 2) now just put <html>		
TEST DETAILS			
REMEDIATION	USE USER INPUT VALIDATION AND WAF		
REFERENCES			

CSRF

CVSS SEVERITY	High		CVSSv3 SCORE	7.1
CVSSv3 CRITERIAS	Attack Vector :	Network	Scope :	Changed
	Attack Complexity :	High	Confidentiality :	High
	Required Privileges :	Low	Integrity :	Low
	User Interaction :	Required	Availability :	Low
AFFECTED SCOPE				
DESCRIPTION	Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts.			
OBSERVATION	Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts.			
TEST DETAILS	 <p>Image 1 - image.png</p>			

 <p>Image 2 - image.png</p>	
REMEDIATION	Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts.
REFERENCES	Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are submitted from a user that the web application trusts.

CLICKJACKING

CVSS SEVERITY	Medium	CVSSv3 SCORE	6.3
CVSSv3 CRITERIAS	Attack Vector : Network Attack Complexity : Low Required Privileges : Low User Interaction : None	Scope : Unchanged Confidentiality : Low Integrity : Low Availability : Low	
AFFECTED SCOPE			
DESCRIPTION	Clickjacking is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information or allowing others to take control of their computer while clicking on seemingly innocuous objects, including web pages. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function. Clickjacking is an instance of the confused deputy problem, a term used to describe when a computer is innocently fooled into misusing its authority.		
OBSERVATION	1)Open any url which you want to test let's say https://www.incrypts.com/ 2) now just put <html>		
TEST DETAILS			
REMEDIATION	Use "X- Frame Options"		
REFERENCES			