Dhatri

VULNERABILITY REPORT

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0		DHATRI	Initial Version

TABLE OF CONTENTS

General Information

Scope

undefined has mandated us to perform security tests on the following scope:

Organisation

The testing activities were performed between undefined and undefined.

EXECUTIVE SUMMARY

VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
Medium	VULN-001	XSS	
Medium	VULN-003	CSRF	

TECHNICAL DETAILS

XSS

CVSS SEVERITY	**Medium**		**CVSSV3 SCORE**	**4.6**
CVSSV3 CRITERIAS	Attack Vector :	**Network**	Scope :	**Unchanged**
	Attack Complexity :	**High**	Confidentiality :	**Low**
	Required Privileges :	**Low**	Integrity :	**Low**
	User Interaction :	**Required**	Availability :	**Low**
AFFECTED SCOPE				
DESCRIPTION	Summary: Stored XSS can be submitted on reports, and anyone who will check the report the XSS will trigger. Description: Stored XSS, also known as persistent XSS, is the more damaging than non-persistent XSS. It occurs when a malicious script is injected directly into a vulnerable web application.			
OBSERVATION	Steps To Reproduce: Go to https://app.mopub.com/reports/custom/ Click New network report. On the name, enter payload: "><img src=x onerror=alert(document.domain)> Click Run and save then XSS will trigger. Demonstration of the vulnerability: PoC: xssed.webm (F412243) Tested on Firefox and chrome.			
TEST DETAILS				
REMEDIATION	The attacker can steal data from whoever checks the report.			
REFERENCES	https://hackerone.com/reports/485748			

CSRF

CVSS SEVERITY	**Medium**		**CVSSV3 SCORE**	**4.5**
CVSSV3 CRITERIAS	Attack Vector :	**Physical**	Scope :	**Unchanged**
	Attack Complexity :	**High**	Confidentiality :	**None**
	Required Privileges :	**Low**	Integrity :	**Low**
	User Interaction :	**Required**	Availability :	**High**
AFFECTED SCOPE				
DESCRIPTION	Cross-site request forgery (also known as CSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform. It allows an attacker to partly circumvent the same origin policy, which is designed to prevent different websites from interfering with each other.			
OBSERVATION	SITE uses the authenticity_token token during login to prevent CSRF. However, the authenticity_token token is not properly verified, so an attacker can log in via CSRF without the authenticity_token token. In other words, Hacker One thinks that it implemented CSRF token through authenticity_token token, but it is not.			
TEST DETAILS				
REMEDIATION	The victim may add sensitive payment information to the attacker's new account			
REFERENCES	https://hackerone.com/reports/834366			