

Veneela

# VULNERABILITY REPORT

---

**MODIFICATIONS HISTORY**

Version	Date	Author	Description
1.0		VENEELA	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 .....	8
4.	Vulnerabilities summary .....	6

---

## 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 : <b>Network</b>	Scope : <b>Unchanged</b>	
	Attack Complexity : <b>High</b>	Confidentiality : <b>Low</b>	
	Required Privileges : <b>Low</b>	Integrity : <b>Low</b>	
	User Interaction : <b>Required</b>	Availability : <b>Low</b>	
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 <a href="https://app.mopub.com/reports/custom/">https://app.mopub.com/reports/custom/</a> 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: <a href="#">xssed.webm (F412243)</a> Tested on Firefox and chrome.		
TEST DETAILS			
REMEDIATION	The attacker can steal data from whoever checks the report.		
REFERENCES	<a href="https://hackerone.com/reports/485748">https://hackerone.com/reports/485748</a>		

## CSRF

CVSS SEVERITY	Medium	CVSSv3 SCORE	4.5
CVSSv3 CRITERIAS	Attack Vector : Physical Attack Complexity : High Required Privileges : Low User Interaction : Required	Scope : Unchanged Confidentiality : None Integrity : Low 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		