

**Name : C NAVEEN**

**Reg.No : 19BCE7028**

Secure Coding Lab Audit

# VULNERABILITY REPORT

SATURDAY, MAY 15, 2021





---

## MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	05/15/2021	C NAVEEN	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 .....	11
4.	Vulnerabilities summary .....	6



---

## GENERAL INFORMATION

---

### SCOPE

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

- Entire infrastructure

---

### ORGANISATION

The testing activities were performed between 05/01/2021 and 05/15/2021.



---

## EXECUTIVE SUMMARY



---

## VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
High	IDX-002	Shell code injection	
High	IDX-001	Buffer overflow	
High	IDX-003	DOM XSS	

## TECHNICAL DETAILS

### SHELL CODE INJECTION

CVSS SEVERITY	High		CVSSv3 SCORE	8.9
CVSSv3 CRITERIAS	Attack Vector :	Network	Scope :	Changed
	Attack Complexity :	Low	Confidentiality :	Low
	Required Privileges :	Low	Integrity :	High
	User Interaction :	Required	Availability :	High
AFFECTED SCOPE				
DESCRIPTION	Shell Code Injection is an attack that consists in executing commands on a victim's operating system via a vulnerable application.			
OBSERVATION	We have identified that this vulnerability can execute different malicious code and even trigger different application including command prompt.			

#### TEST DETAILS

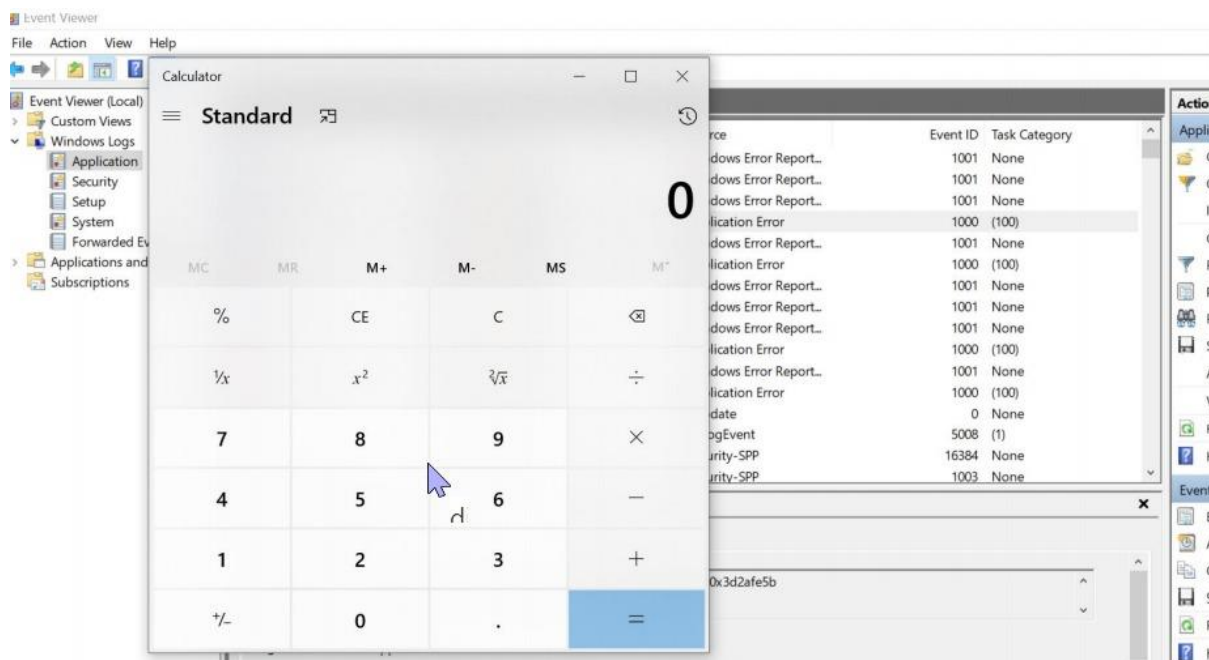


IMAGE 1 – IMAGE.PNG

REMEDIATION	<ul style="list-style-type: none"> <li>Addressing buffer overflow vulnerability.</li> <li>Input sanitization.</li> <li>Input validation (we may use regular expressions for validation).</li> <li>Implementing ASLR, DEP, SEH.</li> </ul>
-------------	---



<b>REFERENCES</b>	<a href="https://www.httpcs.com/en/php-shell-code-injection-vulnerability#:~:text=Shell%20Code%20Injection%20is%20an,system%20via%20a%20vulnerable%20aplication.">https://www.httpcs.com/en/php-shell-code-injection-vulnerability#:~:text=Shell%20Code%20Injection%20is%20an,system%20via%20a%20vulnerable%20aplication.</a>
-------------------	---



## BUFFER OVERFLOW

CVSS SEVERITY	High		CVSSv3 SCORE	8.9
CVSSv3 CRITERIAS	Attack Vector : <b>Network</b>	Scope : <b>Changed</b>	Attack Complexity : <b>Low</b>	Confidentiality : <b>High</b>
	Required Privileges : <b>Low</b>	Integrity : <b>Low</b>	User Interaction : <b>Required</b>	Availability : <b>High</b>
AFFECTED SCOPE				
DESCRIPTION	In a buffer overflow attack, the extra data includes instructions that are intended to trigger damaging activities such as corrupting files, changing data, sending private information across the internet, etc. An attacker would simply take advantage of any program which is waiting for certain user input and inject surplus data into the buffer.			
OBSERVATION	We have observed that buffer overflow potentially crash an application and unknowingly allows command injection attacks.			

### TEST DETAILS

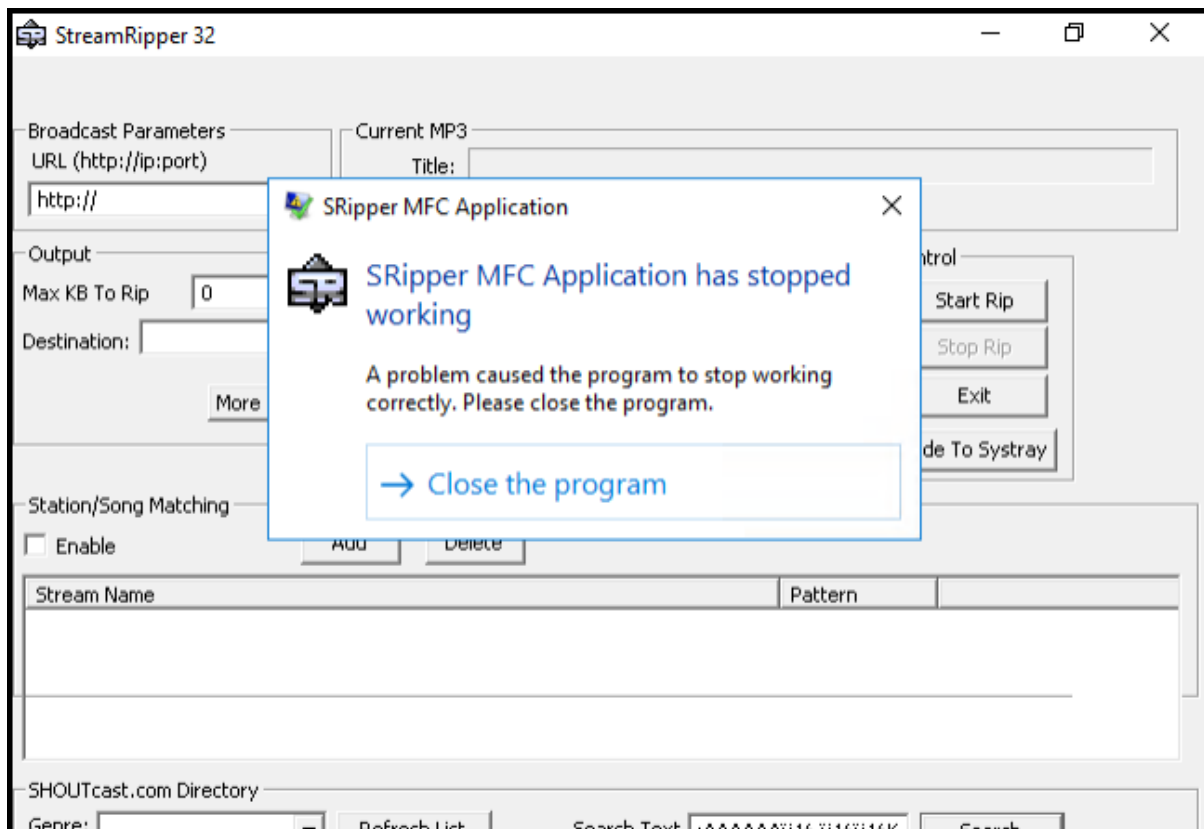


IMAGE 2 – IMAGE.PNG



<b>REMEDIATION</b>	<ul style="list-style-type: none"><li>• ASLR</li><li>• DEP</li><li>• SEHOP</li></ul>
<b>REFERENCES</b>	<a href="http://www.cloudflare.com/learning/security/threats/buffer-overflow/">www.cloudflare.com/learning/security/threats/buffer-overflow/</a>



## DOM XSS

CVSS SEVERITY	High		CVSSv3 SCORE	7.6
CVSSv3 CRITERIAS	Attack Vector :	Network	Scope :	Changed
	Attack Complexity :	Low	Confidentiality :	High
	Required Privileges :	Low	Integrity :	Low
	User Interaction :	Required	Availability :	None
AFFECTED SCOPE				
DESCRIPTION	DOM XSS stands for Document Object Model-based <b>Cross-site Scripting</b> . ... All HTML documents have an associated <b>DOM</b> 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 <b>DOM</b> of the HTML page where the script runs.			
OBSERVATION	<div>1)Open any url which you want to test let's say https://www.incrypts.com/ 2) now just put &lt;html&gt;</div>			
TEST DETAILS				
REMEDIATION	USE USER INPUT VALIDATION AND WAF			
REFERENCES				



CONFIDENTIAL