



CSE-2010 Secure Coding Lab-12

Name :- Tarun Kashyap

Reg. No. :- 18BCD7183

Secure Coding Lab Audit

VULNERABILITY REPORT

SATURDAY, MAY 15, 2021



CONFIDENTIAL MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	05/15/2021	Tarun Kashyap	Initial Version

2 / 12



CONFIDENTIAL

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	



CONFIDENTIAL

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.



CONFIDENTIAL

EXECUTIVE 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	

6 / 12



CONFIDENTIAL 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

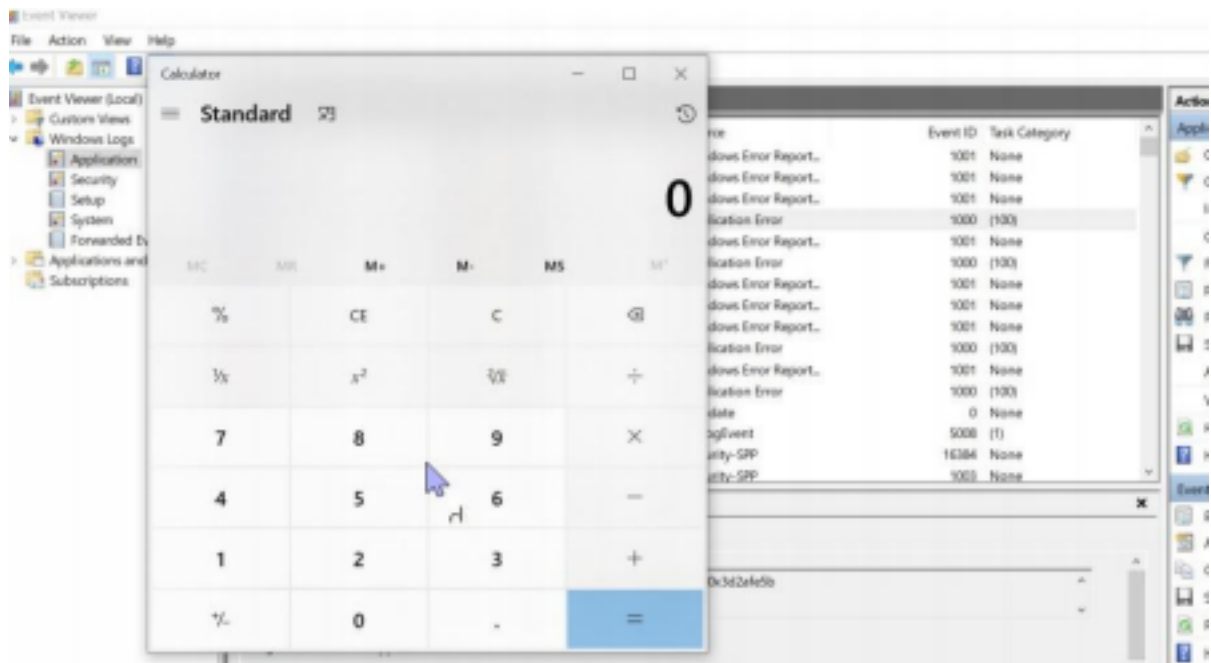


Image 1 – image.png

REMEDIATION

- Addressing buffer overflow vulnerability.
- Input sanitization.
- Input validation (we may use regular expressions for validation).
- Implementing ASLR, DEP, SEH.

7 / 12



CONFIDENTIAL

REFERENCES

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

8 / 12



CONFIDENTIAL

BUFFER OVERFLOW

CVSS SEVERITY	High	CVSSv3 SCORE	8.9
---------------	------	--------------	-----

CVSSv3 CRITERIAS	<p>Attack Vector : Network Scope : Changed Attack Complexity : Low</p> <p>Confidentiality : High</p> <p>Required Privileges : Low Integrity : Low</p> <p>User Interaction : Required Availability : High</p>
AFFECTED SCOPE	
DESCRIPTION	<p>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.</p>
OBSERVATION	<p>We have observed that buffer overflow potentially crash an application and unknowingly allows command injection attacks.</p>

TEST DETAILS

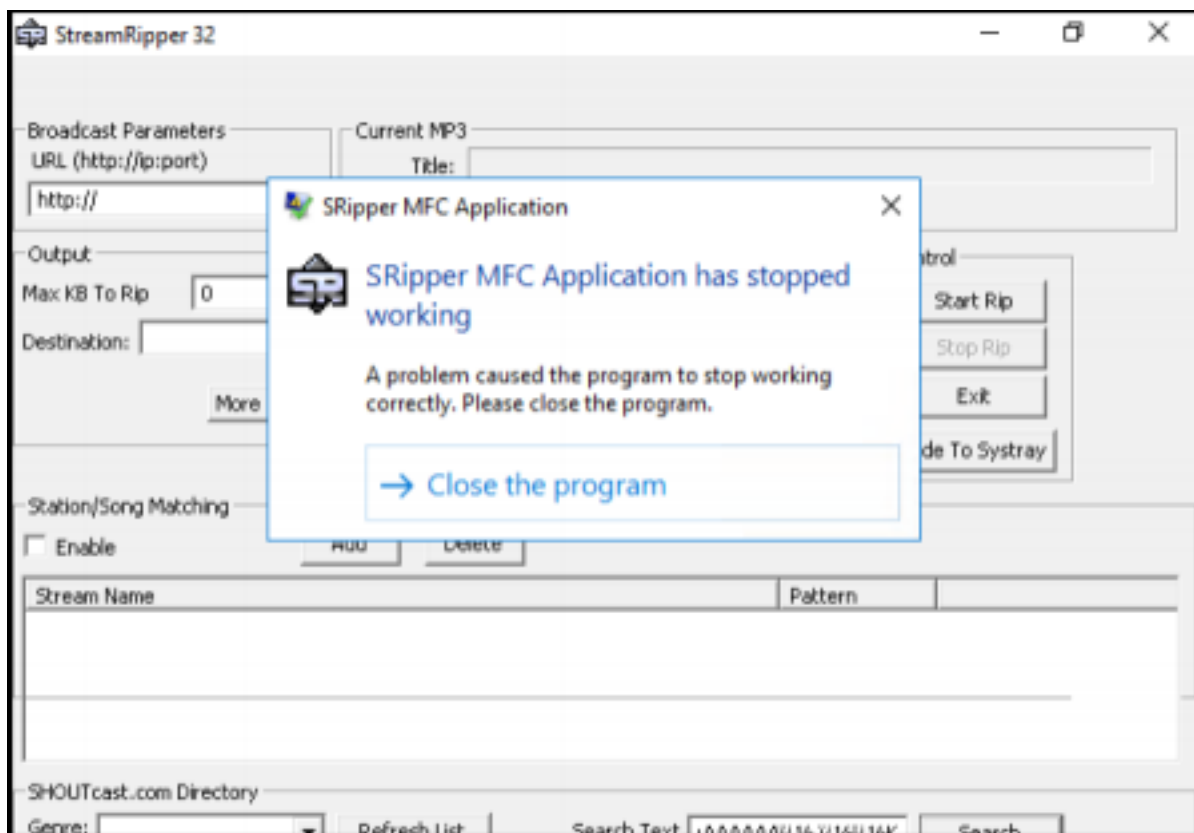


Image 2 – image.png



REMEDIATION	<ul style="list-style-type: none"> • ASLR • DEP • SEHOP
--------------------	--

REFERENCES	www.cloudflare.com/learning/security/threats/buffer-overflow/
------------	---

10 / 12



CONFIDENTIAL

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 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			

11 / 12

