CSE-2010 Secure Coding Lab-12

Name :- Amritmoy Pain

Reg. No. :- 18BCE7344

Secure Coding Lab Audit

VULNERABILITY REPORT

SATURDAY, MAY 15, 2021

 MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	05/20/2021	Amritmoy Pain	Initial Version

TABLE OF CONTENTS

GENERAL INFORMATION

SCOPE

VIT Amravathi 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.

CONFIDENTIALVULNERABILITIESSUMMARY

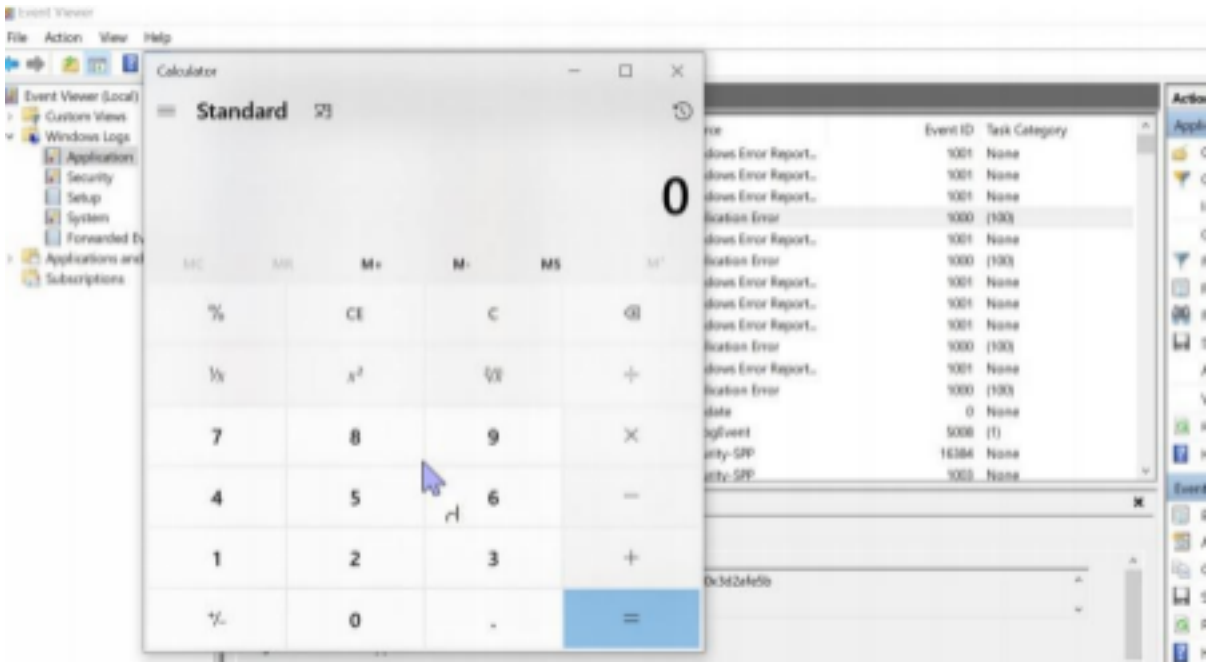
Following vulnerabilities have been discovered:

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

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.

REFERENCES	https://www.httpcs.com/en/php-shell-code-injection vulnerability#:~:text=Shell%20Code%20Injection%20is%20an,system%20via%20a%20vulnerable %2 0ap plication.

BUFFER OVERFLOW

CVSS SEVERITY		**High CVSSV3 SCORE**	**8.9**

CVSSv3 CRITERIAS	Attack Vector : **Network** Scope : **Changed** Attack Complexity : **Low** Confidentiality : **High** Required Privileges : **Low** Integrity : **Low** User Interaction : **Required** Availability : **High**
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

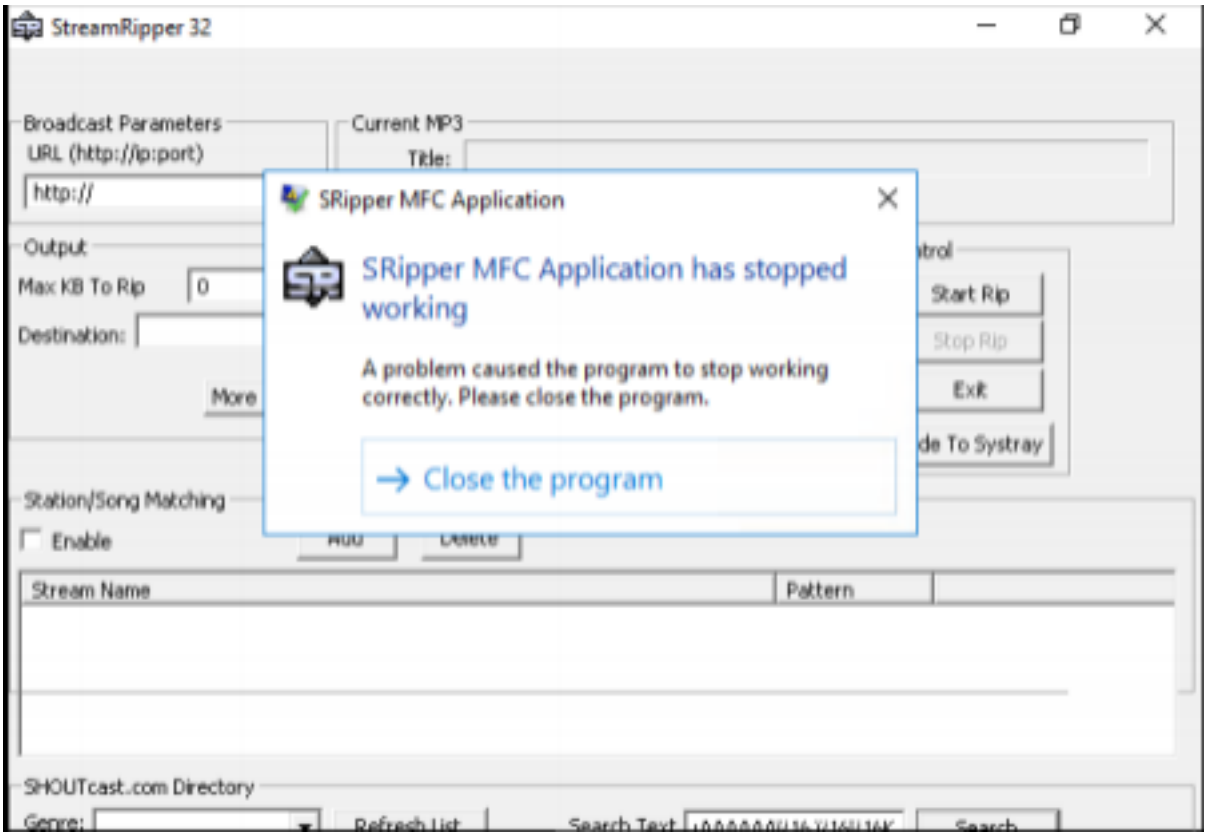


Image 2 – image.png

REMEDIATION · ASLR
· DEP
· SEHOP

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


 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 **References**	USE USER INPUT VALIDATION AND WAF