Secure Coding (CSE2010)

LAB Experiment 13

Done by,

Aadil Mohammed

Reg.No: 19BCI7052

Slot: L23+L24

Aadil Mohammed

VULNERABILITY REPORT

FRIDAY, JUNE 11,2021

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	11-06-2021	Aadil Mohammed	Initial Version

TABLE OF CONTENTS

General Information

Scope

Prof. Sibi Chakkaravarthy S has mandated us to perform security tests on the following scope:

- Lab 7 to Lab 11 experiments

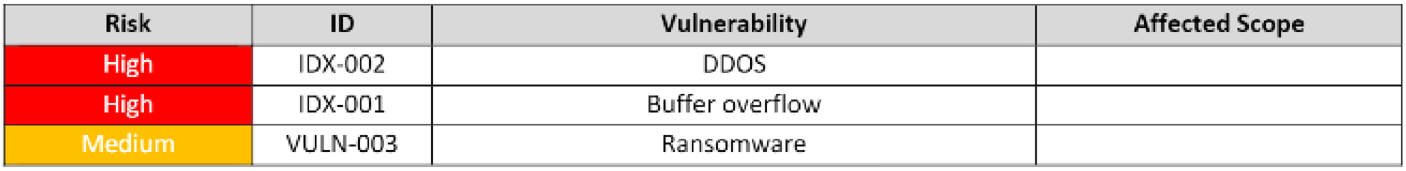
Organisation

The testing activities were performed between 11-06-2021 and 11-06-2021.

Executive Summary{#summary}

VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:



Risk	ID	Vulnerability	Affected Scope
High	IDX-002	DDOS	
High	IDX-001	Buffer overflow	
Medium	VULN-003	Ransomware	

Technical Details{#findings}

DDOS

CVSS Severity	**High**		CVSSv3 Score	**8.3**
CVSSv3 criterias	Attack Vector :	**Network**	Scope :	**Changed**
	Attack Complexity :	**High**	Confidentiality :	**High**
	Required Privileges :	**None**	Integrity :	**High**
	User Interaction :	**Required**	Availability :	**High**
Affected scope				
Description	This is used to crash a website using multiple pinging			
Observation				
Test details				
Remediation				
References				

Buffer overflow

CVSS Severity	**High**		**CVSSv3 Score**	**8.3**
CVSSv3 criterias	Attack Vector :	**Network**	Scope :	**Changed**
	Attack Complexity :	**High**	Confidentiality :	**High**
	Required Privileges :	**High**	Integrity :	**High**
	User Interaction :	**Required**	Availability :	**High**
Affected scope				
Description	This is a code level error normally made by humans due to the type casting errors. It leads to the crass of rocket ariane-5.			
Observation	This is done using steam ripper			
Test details				
Remediation				
References				

CVSS Severity	**Medium**		**CVSSv3 Score**	**6.2**
CVSSv3 **criterias**	Attack Vector :	**Physical**	Scope :	**Unchanged**
	Attack Complexity :	**High**	Confidentiality :	**High**
	Required Privileges :	**Low**	Integrity :	**High**
	User Interaction :	**Required**	Availability :	**High**
Affected scope				
Description	This is used to infect the navie windows to get the ransom.			
Observation				
Test details				
Remediation				
References				