

## Secure Coding Lab - 8

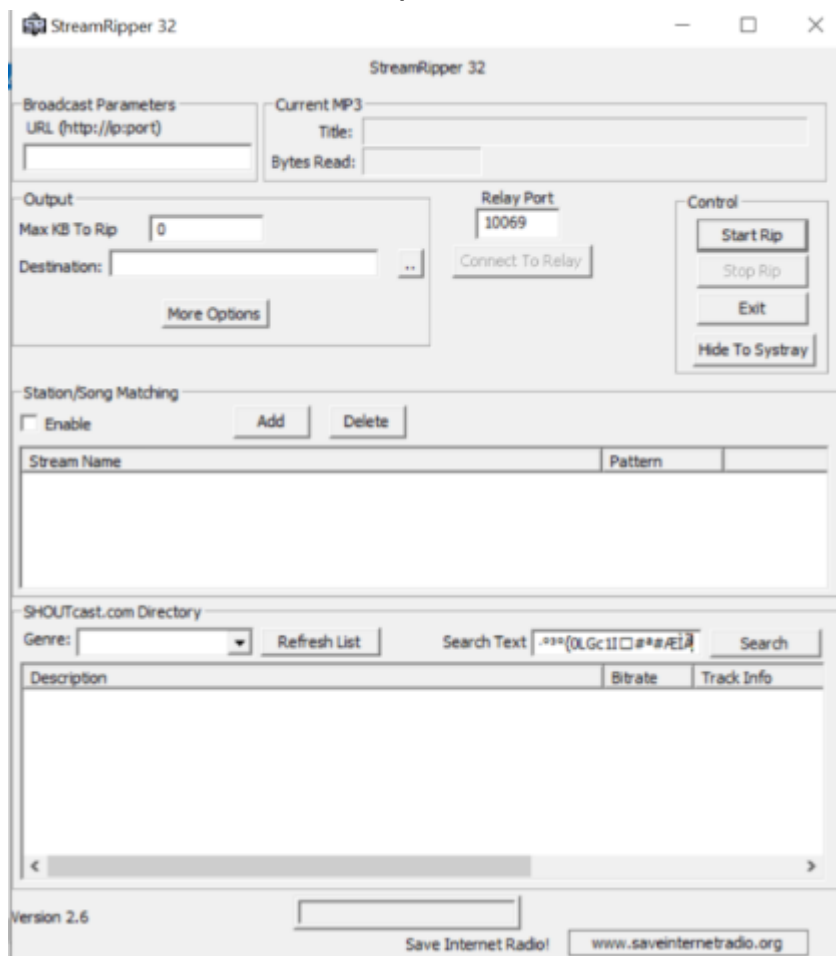
Name: Charitha Bodapothula

Reg.No: 19BCN7005

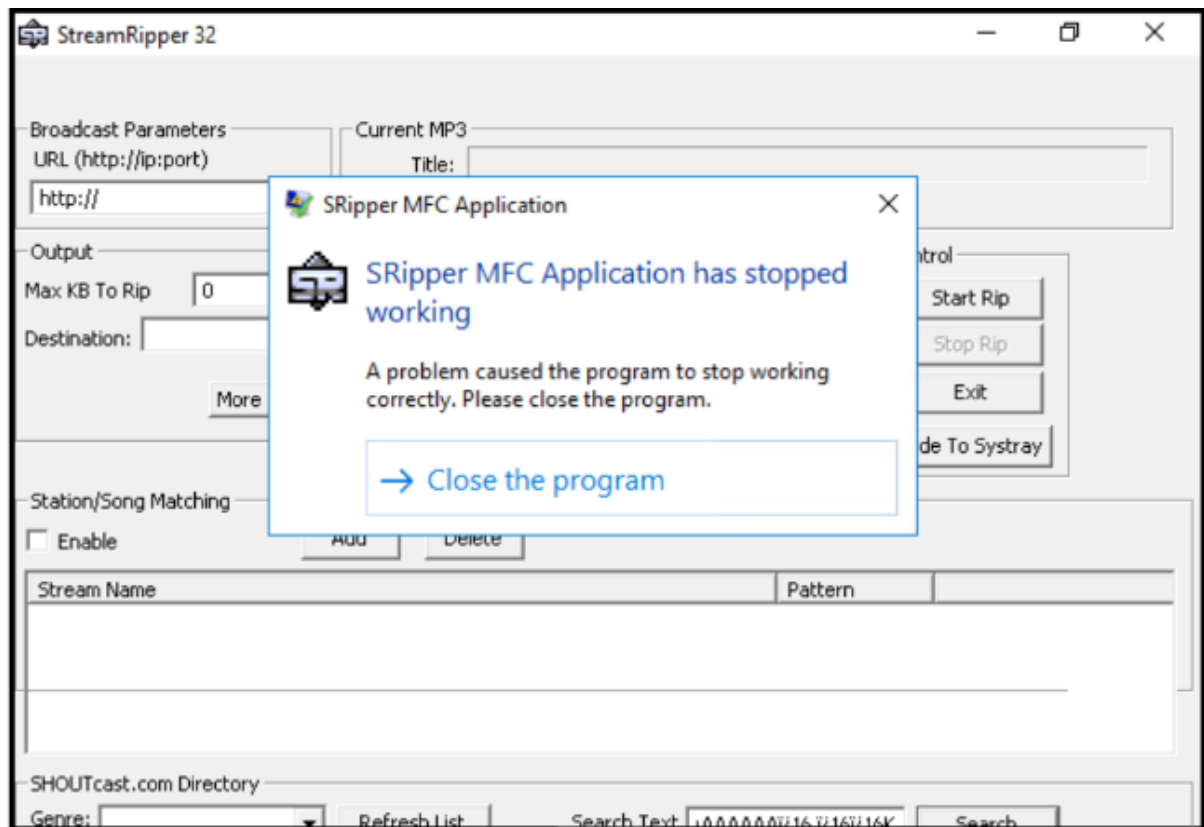
Slot: L23+24

Run the python exploit2.py

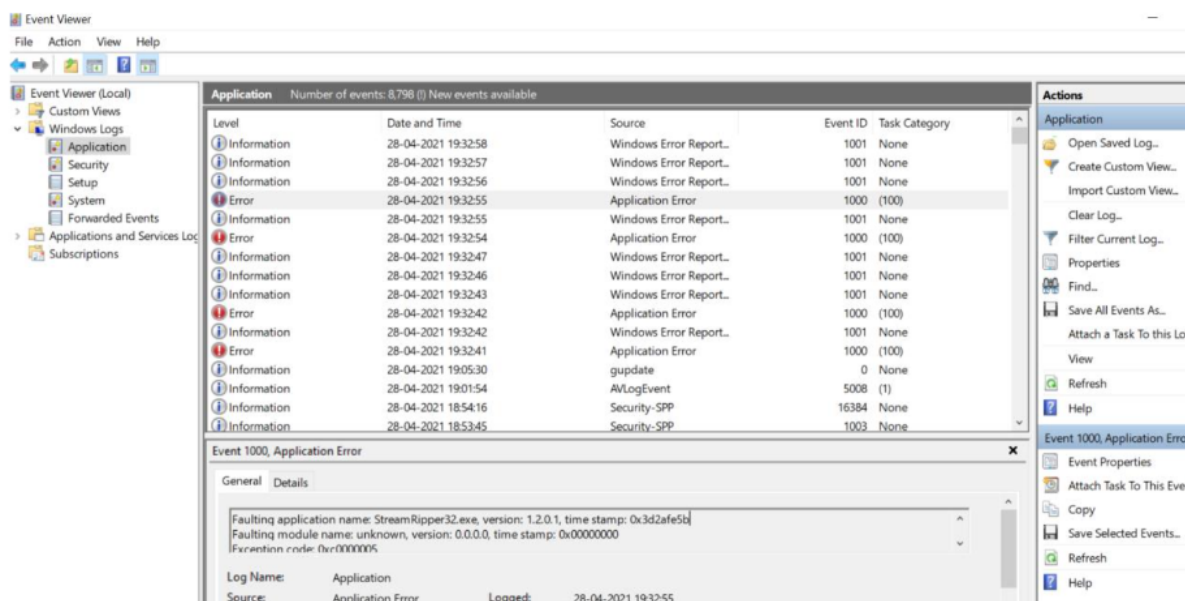
And then install StreamRipper32 and paste the payload in the search box, select the search option.



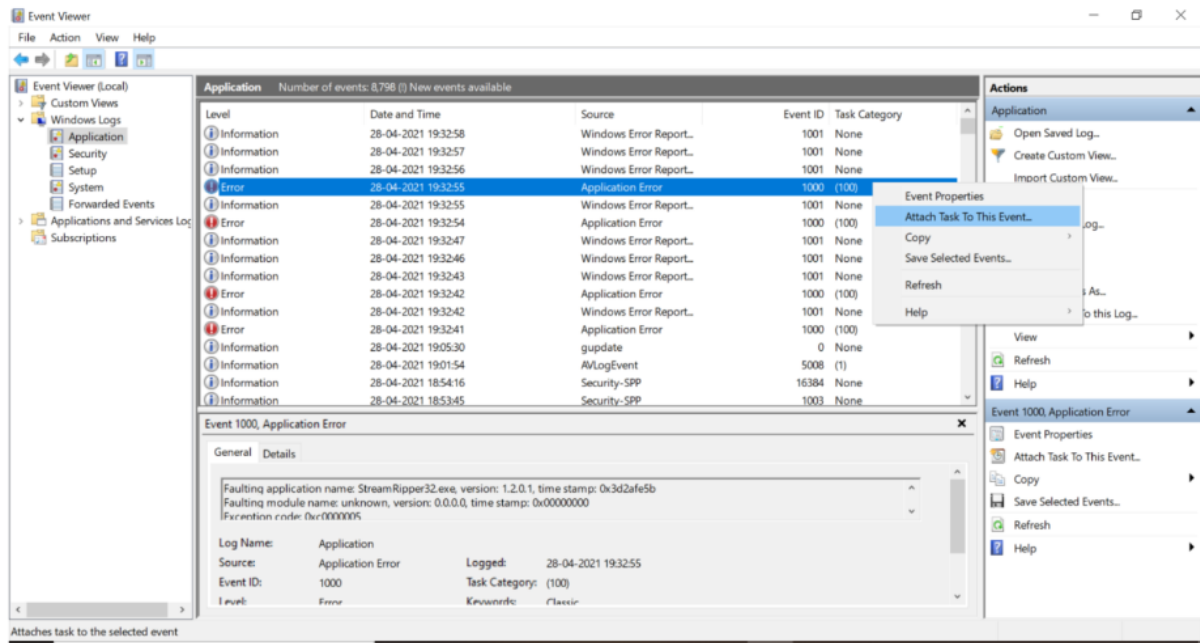
The application gets crashed by exploiting buffer overflow



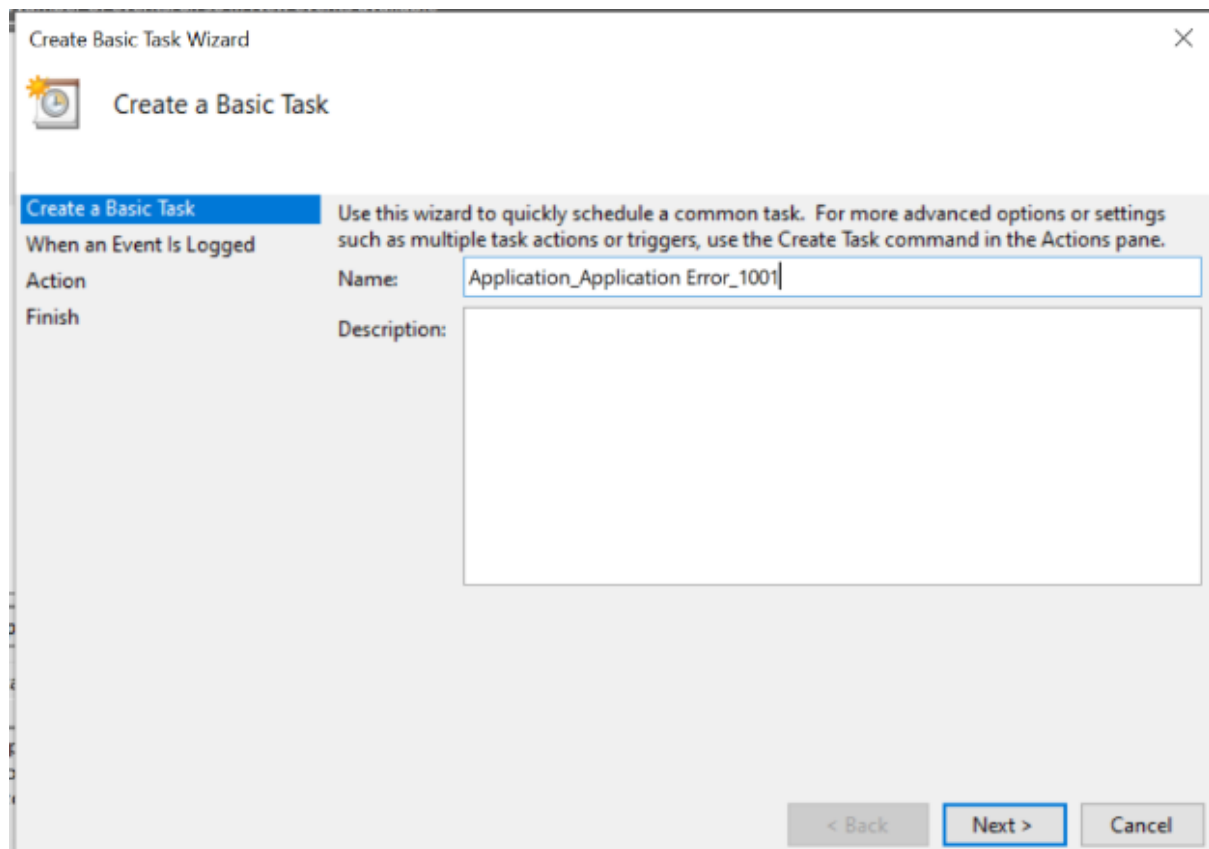
Go to the event viewer



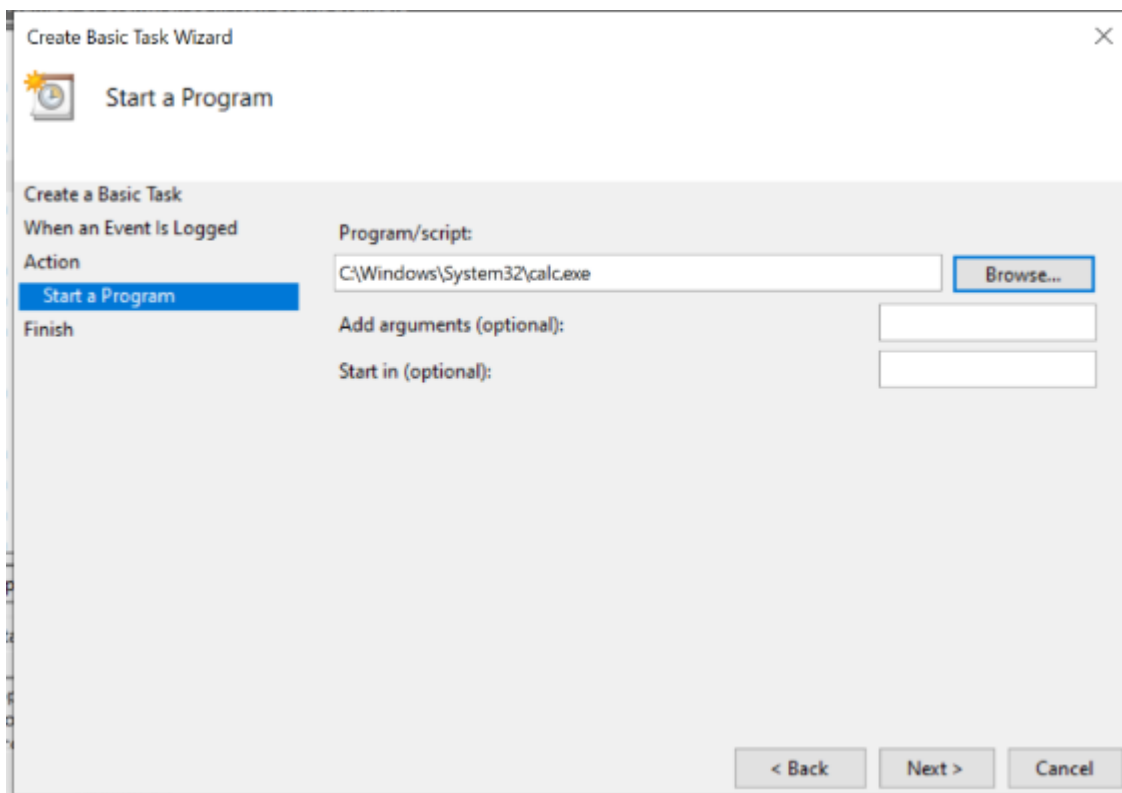
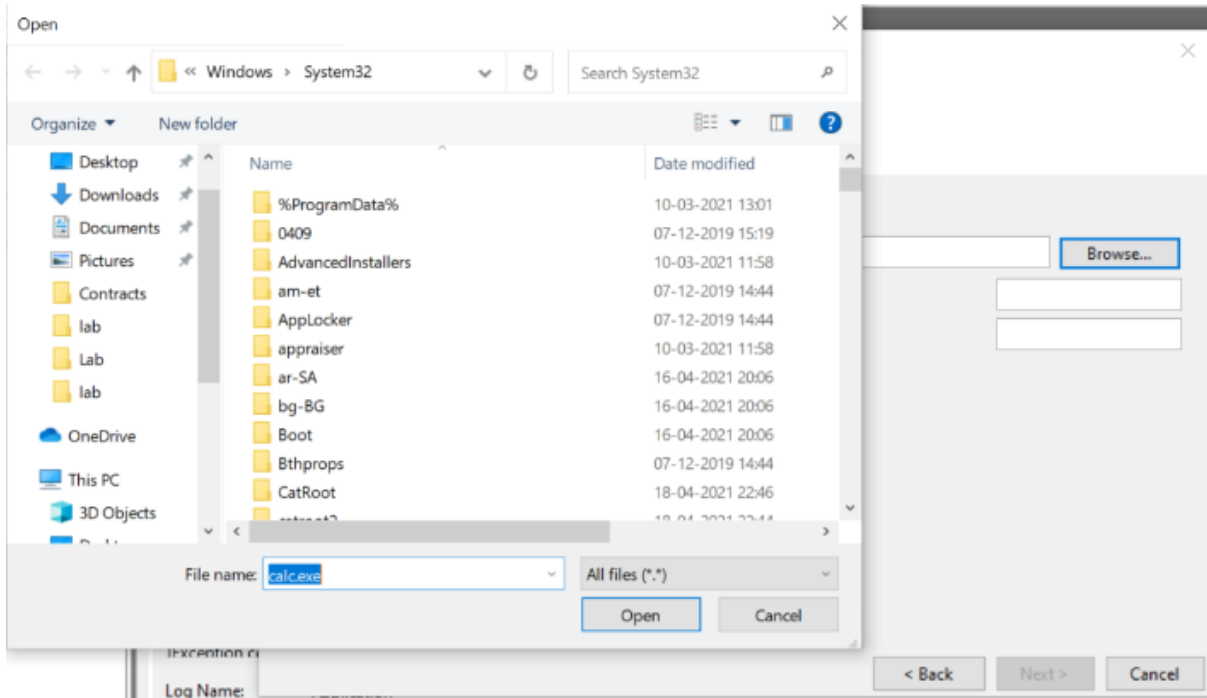
Then, right-click the error and select attach task to this event




Create a task:



Select calc.exe and put it in the default trigger on crash



Create Basic Task Wizard

 Summary

Create a Basic Task

When an Event Is Logged

Action

Start a Program

Finish

Name: Application\_Application Error\_1001

Description:

Trigger: On an event; On event - Log: Application, Source: Application Error, Event ID: 1001

Action: Start a program; C:\Windows\System32\calc.exe

☐ Open the Properties dialog for this task when I click Finish

When you click Finish, the new task will be created and added to your Windows schedule.

< Back Finish Cancel

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Logs
- Subscriptions

Level	Date and Time	Source	Event ID	Task Category
Information	28-04-2021 19:32:58	Windows Error Report...	1001	None
Information	28-04-2021 19:32:57	Windows Error Report...	1001	None
Information	28-04-2021 19:32:56	Windows Error Report...	1001	None
Error	28-04-2021 19:32:55	Application Error	1000 (100)	
Information	28-04-2021 19:32:55	Windows Error Report...	1001	None
Error	28-04-2021 19:32:54	Application Error	1000 (100)	
Information	28-04-2021 19:32:47	Windows Error Report...	1001	None
Information	28-04-2021 19:32:46	Windows Error Report...	1001	None
Information	28-04-2021 19:32:43	Windows Error Report...	1001	None
Error	28-04-2021 19:32:42	Application Error	1000 (100)	
Information	28-04-2021 19:32:42	Windows Error Report...	1001	None
Error	28-04-2021	Event Viewer	1000 (100)	
Information	28-04-2021		0	None
Information	28-04-2021		1008 (1)	
Information	28-04-2021		384	None
Information	28-04-2021		1003	None

Event 1000, Application Error

General Details

Faulting application name: StreamRipper32.exe, version: 1.2.0.1, time stamp: 0x3d2afe5b  
 Faulting module name: unknown, version: 0.0.0.0, time stamp: 0x00000000  
 Exception code: 0xc0000005

Event Viewer created the Scheduled Task Application\_Application Error\_1001. To modify the task, open Task Scheduler.

OK

Now the task has been created.  
 Put the payload in StreamRipper32

StreamRipper 32

Broadcast Parameters

URL (http://p:port)

Current MP3

Title:

Bytes Read:

Output

Max KB To Rip

0

Destination:

..

More Options

Relay Port

10069

Connect To Relay

Control

Start Rip

Stop Rip

Exit

Hide To Systray

Station/Song Matching

☐ Enable

Add

Delete

Stream Name	Pattern
-------------	---------

SHOUTcast.com Directory

Genre:

Refresh List

Search Text

DF3K0XUQsrMCTS0AA

Search

Description	Bitrate	Track Info
-------------	---------	------------

Event Viewer

File Action View Help

Event Viewer (Local)

Custom Views

Windows Logs

Application

Security

Setup

System

Forwarded Events

Applications and Subscriptions

Standard

MC MR M+ M- MS M\*

%

CE

C

1/x

$x^2$

$\sqrt[3]{x}$

$\div$

7

8

9

$\times$

4

5

6

-

1

2

3

+

$\pm/\%$

0

.

=

Source	Event ID	Task Category
Windows Error Report...	1001	None
Windows Error Report...	1001	None
Windows Error Report...	1001	None
Application Error	1000	(100)
Windows Error Report...	1001	None
Application Error	1000	(100)
Windows Error Report...	1001	None
Windows Error Report...	1001	None
Windows Error Report...	1001	None
Application Error	1000	(100)
Windows Error Report...	1001	None
Application Error	1000	(100)
date	0	None
pgEvent	5008	(1)
urity-SPP	16384	None
urity-SPP	1003	None

0x3d2afe5b

Actions

Application

Oper

Creat

Impo

Clear

Filter

Propri

Find...

Save

Attac

View

Refre

Help

Event 100

Even

Attac

Copy

Save

Refre

Help