Deakin Detonator Tool Kit – Bug Report

Sections

Contents

Bug 1 - MsfConsole Listening Tool in Reverse TCP Shell AV

Bug ID: B0001

Bug Name: Application crashes upon clicking the 'Start Listening' button when awaiting connection from victim in MsfConsole Listening Tool for Reverse TCP Shell attack vector.

Area Path: PT-GUI -> ExecutionTools -> MsfconsoleListener.py

Build Number: Version Number 5.0.1

Environment: Kali Linux Version 2022.1

Severity (High/Medium/Low): HIGH

Priority(High/Medium/Low): HIGH

Assigned to: Unassigned

Reported By: Kawthar

Reported On: 28/04/2022

Status (New/Open/Active): Open

Description:

Application crashes after clicking the 'Start Listening' button in step 2 of the Reverse TCP Shell attack vector (MsfConsole Listening Tool). The error messages are not executed and the application freezes and becomes unresponsive requiring a forced shutdown of the application in from the terminal, or crashes. The payload file .exe cannot be run on Linux without a wine application and application still crashes after not receiving a response within a few seconds.

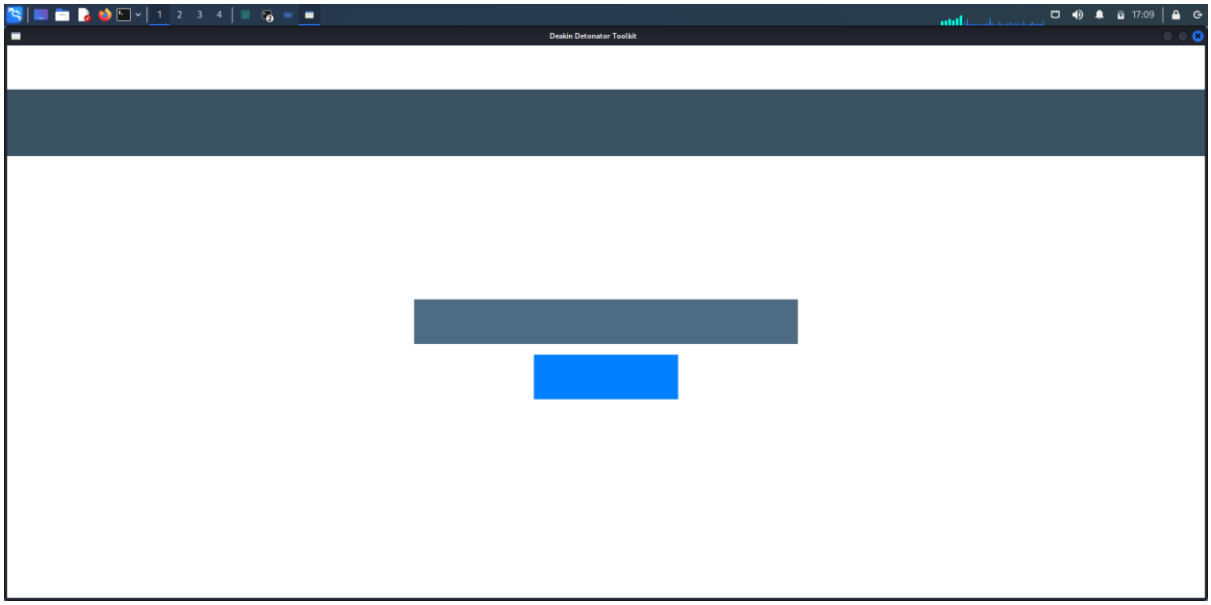
Steps to Reproduce:

1) Run the application in terminal
2) Open the Atack Vectors Page
3) Launch the Reverse TCP Shell Attack Vector
4) Click Step 1 -> Payload Generator Tool button -> Launch Field button -> Yes to confirm the correct IP address (10.0.2.15) -> Yes to confirm default port (4444) -> Save Payload -> Generate Payload -> Launch Tool
5) Navigate to Step 2 by using the navigation bar (Attack Vectors -> Reverse TCP Shell -> Step 2)
6) Open Listener Tool -> Confirm default IP address -> Confirm default port (4444) -> Start Listening
7) Try executing payload in terminal (not possible without using an application like Wine)
8) Open the application
9) See blank or frozen page
10) Try and exit
11) Force close or force refresh in terminal
12) See error codes in terminal like below

Expected Result: Upon clicking the ‘Start Listening’ button, you should be able to run the payload .exe file and be prompted to a successful message “Connection successful”, or be unable to run the .exe file and receive the unsuccessful messages “ [Errno 111] Connection refused”, or “Max retries exceeded with url: /api/.”

Terminal Error message:

- File "/usr/lib/python3/dist-packages/requests/adapters.py", line 516, in send raise ConnectionError(e, request=request) requests.exceptions.ConnectionError: HTTPConnectionPool(host='127.0.0.1', port=55553):
  Max retries exceeded with url: /api/ (Caused by NewConnectionError('<urllib3.connection.HTTPConnection object at 0x7fef603d09a0>: Failed to establish a new connection: [Errno 111] Connection refused'))
- File "/usr/lib/python3.9/tkinter/__init__.py", line 1892, in __call__
  return self.func(*args)
  File "/home/user/PT-GUI/ExecutionTools/MsfconsoleListener.py", line 82, in <lambda>
  command=lambda: session_interact())
  File "/home/user/PT-GUI/ExecutionTools/MsfconsoleListener.py", line 269, in session_interact
  time.sleep(0.1)



Bug 2 – Directory Traversal & IDOR

Bug ID: B0002

Bug Name: Application froze after auto scanning for directories in the Directory Traversal Fizzer Attack Vector and needed to be rebooted.

Area Path: PT-GUI -> Fuzzers -> DirectoryTraversalFuzzer.py

Build Number: Version Number 5.0.1

Environment: Kali Linux Version 2022.1

Severity (High/Medium/Low): HIGH

Priority(High/Medium/Low): HIGH

Assigned to: Unassigned

Reported By: Kawthar

Reported On: 09/05/2022

Status (New/Open/Active): Open

Description:

Application freezes after clicking the 'Start Library Scan' button in step 2 of the Directory Traversal & IDOR Attack Vector. There are no error messages saying that the website cannot be reached, does not have any other directories, or that the directories found cannot be displayed.

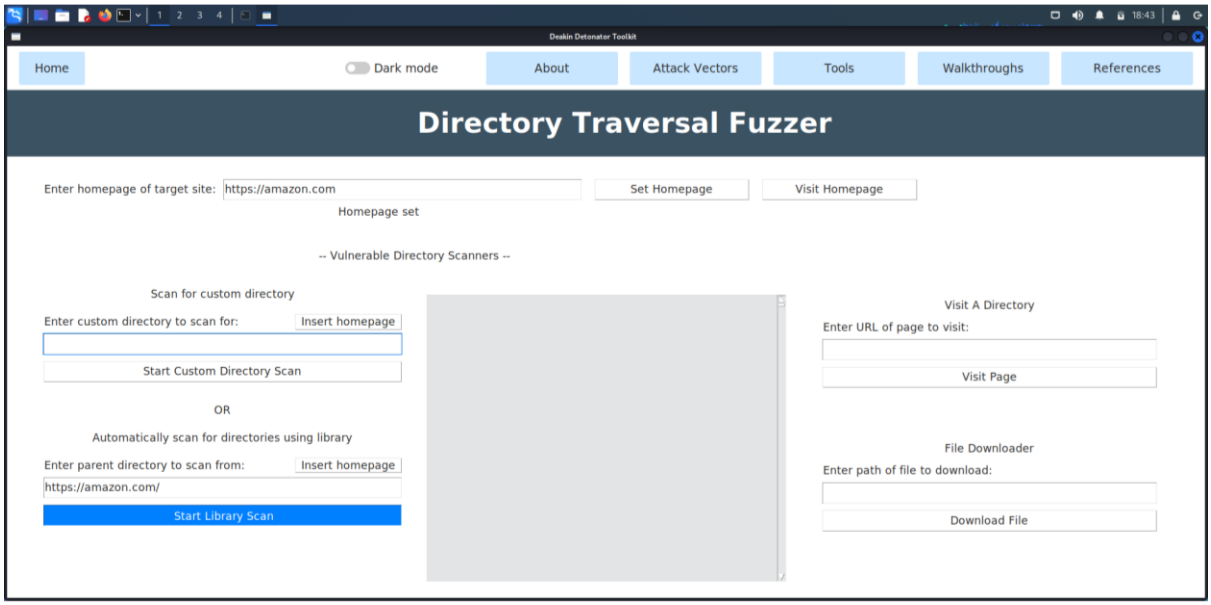
Steps to Reproduce:

1) Run the application in terminal
2) Open the Atack Vectors Page
3) Launch the Directory Traversal & IDOR Attack Vector
4) Click Step 1 -> Directory Traversal Fuzzer button
5) Enter target homepage URL including http or https
6) Set Home Page
7) Insert Homepage into Automatic scanner tool using Insert homepage button and Start Library Scan
8) Wait for any action
9) See Application is frozen
10) Try and exit
11) Force close or force refresh in terminal
12) See error codes in terminal like below

Expected Result: Upon clicking the 'Start Library Scan' button, you should be able to see the other directories available for the website in the output textbox in the middle of the page or see a message of "no other directories found".

Terminal Error message:

```
└─$ python3 main.py
^CException in Tkinter callback
Traceback (most recent call last):
  File "/usr/lib/python3.9/tkinter/__init__.py", line 1892, in __call__
    return self.func(*args)
  File "/home/kohas/PT-GUI/Fuzzers/DirectoryTraversalFuzzer.py", line 137, in <lambda>
    command=lambda: self.library_scan()).place(rely=0.83, relx=0.03, relheight=0.04, relwidth=0.30)
  File "/home/kohas/PT-GUI/Fuzzers/DirectoryTraversalFuzzer.py", line 238, in library_scan
    request = requests.get(command + directory)
  File "/usr/lib/python3/dist-packages/requests/api.py", line 76, in get
    return request('get', url, params=params, **kwargs)
  File "/usr/lib/python3/dist-packages/requests/api.py", line 61, in request
    return session.request(method=method, url=url, **kwargs)
  File "/usr/lib/python3/dist-packages/requests/sessions.py", line 542, in request
    resp = self.send(prep, **send_kwargs)
  File "/usr/lib/python3/dist-packages/requests/sessions.py", line 655, in send
    r = adapter.send(request, **kwargs)
  File "/usr/lib/python3/dist-packages/requests/adapters.py", line 439, in send
    resp = conn.urlopen(
  File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line 699, in urlopen
    httplib_response = self._make_request(
  File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line 382, in _make_request
    self._validate_conn(conn)
  File "/usr/lib/python3/dist-packages/urllib3/connectionpool.py", line 1012, in _validate_conn
    conn.connect()
  File "/usr/lib/python3/dist-packages/urllib3/connection.py", line 411, in connect
    self.sock = ssl_wrap_socket(
  File "/usr/lib/python3/dist-packages/urllib3/util/ssl_.py", line 449, in ssl_wrap_socket
    ssl_sock = _ssl_wrap_socket_impl(
  File "/usr/lib/python3/dist-packages/urllib3/util/ssl_.py", line 493, in _ssl_wrap_socket_impl
    return ssl_context.wrap_socket(sock, server_hostname=server_hostname)
  File "/usr/lib/python3.9/ssl.py", line 500, in wrap_socket
    return self.sslsocket_class._create(
  File "/usr/lib/python3.9/ssl.py", line 1040, in _create
    self.do_handshake()
  File "/usr/lib/python3.9/ssl.py", line 1309, in do_handshake
    self._sslobj.do_handshake()
KeyboardInterrupt
```



Bug 3 – Apache WebServer Exploit

Bug ID: B0003

Bug Name: The code file for the Apache Webserver exploit tool cannot be found therefore the exploit can't be run.

Area Path: PT-GUI -> ATTACKVECTOR -> attackvector8.py

Build Number: Version Number 5.0.1

Environment: Kali Linux Version 2022.1

Severity (High/Medium/Low): HIGH

Priority(High/Medium/Low): HIGH

Assigned to: Unassigned

Reported By: Kawthar

Reported On: 09/05/2022

Status (New/Open/Active): Open

Description:

Application crashes after clicking the 'Launch Exploit' button in step 2 of the Apache WebServer Exploit Attack Vector. The file for tool is missing and causes this crash.

Steps to Reproduce:

1) Run the application in terminal
2) Open the Atack Vectors Page
3) Launch the Apache WebServer Exploit Attack Vector
4) Click Step 1 -> Launch Listener button
5) See the open listening shell
6) Click Step 2 -> Launch Exploit button
7) Application closes
8) See the following error code in terminal

Expected Result: Upon clicking the 'Launch Exploit' button, you should be able to see a shell terminal open up and enter the IP address and port to listen in on.

Terminal Error message:

- Exception in Tkinter callback
  Traceback (most recent call last):
  File "/usr/lib/python3.9/tkinter/__init__.py", line 1892, in __call__return self.func(*args)
  File "/home/kohas/Documents/PT-GUI/ATTACKVECTOR/attackvector8.py", line 42, in load_exploit
  os.chdir("./Tools")
  FileNotFoundError: [Errno 2] No such file or directory: './Tools'

Bug 4 – Walkthrough Video Continues after closing

Bug ID: B0004

Bug Name: The video's audio continues playing after the player is closed

Area Path: PT-GUI -> resources -> Videos

Build Number: Version Number 5.0.1

Environment: Kali Linux Version 2022.1

Severity (High/Medium/Low): LOW

Priority(High/Medium/Low): LOW

Assigned to: Unassigned

Reported By: Kawthar

Reported On: 18/05/2022

Status (New/Open/Active): Open

Description:

The video player continues to play the video audio in the Walkthroughs section for a few seconds after the video player window was closed.

Steps to Reproduce:

1) Run the application in terminal
2) Open the Walkthroughs Page
3) Play the Buffer Overflow video
4) Close the video player using the exit button
5) Listen to the video play for at least 3 seconds after the window is no longer in view

Expected Result: Upon clicking the 'X button for the video player, you should be able no longer see or hear the video playing.

No Terminal Error Message or Screenshot available.

Bug 5 – Dark Mode Header Error

Bug ID: B0005

Bug Name: After turning on Dark Mode and turning it off, the headers for all pages are not returned to their previous colour and there is a pixel that obstructs some letters.

Area Path: PT-GUI -> theme

Build Number: Version Number 5.0.1

Environment: Kali Linux Version 2022.1

Severity (High/Medium/Low): LOW

Priority(High/Medium/Low): LOW

Assigned to: Unassigned

Reported By: Kawthar

Reported On: 18/05/2022

Status (New/Open/Active): Open

Description:

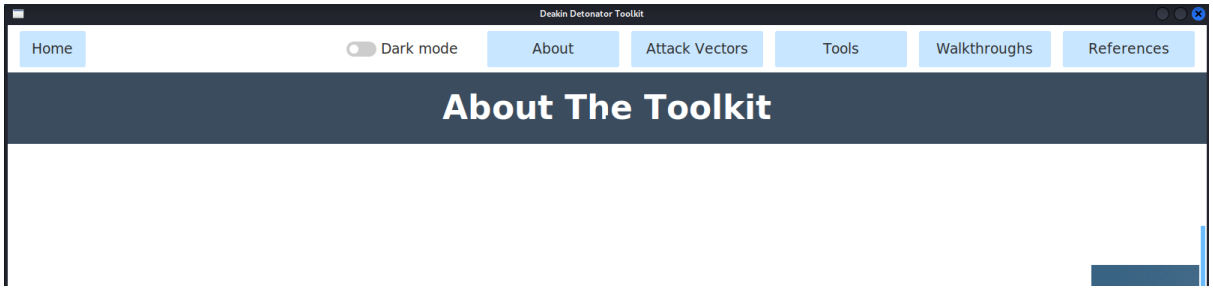
After turning on Dark Mode and turning it off, the headers for all pages are in a dark grey colour unlike the white colour it was before turning Dark Mode on and off. The header also has a pixel cutting off a letter.

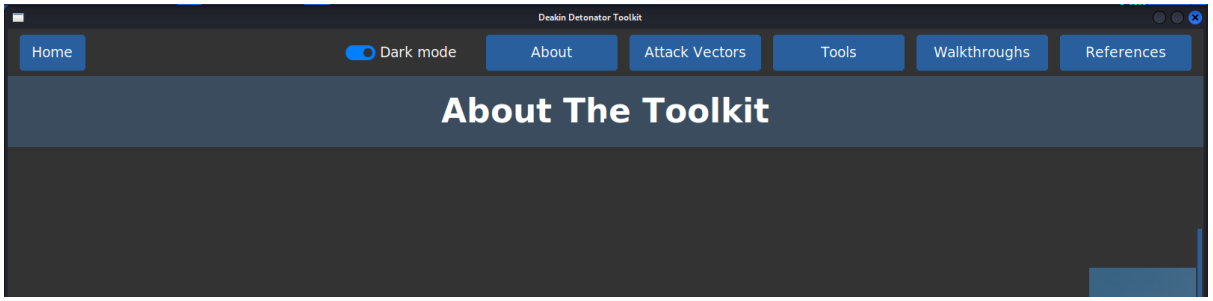
Steps to Reproduce:

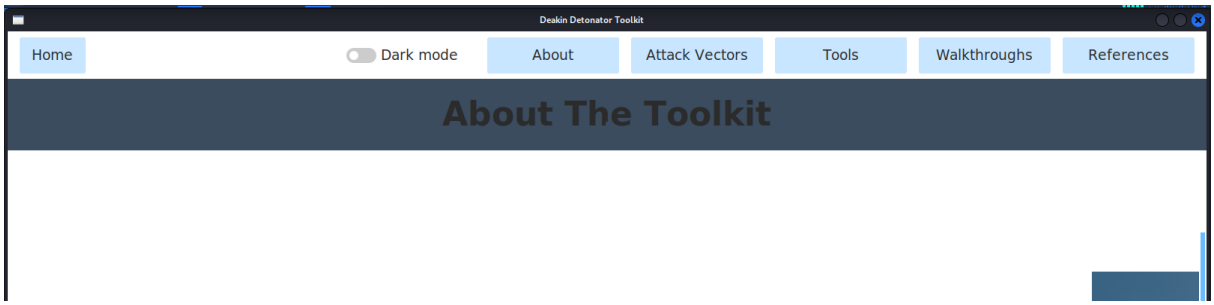
1) Run the application in terminal
2) Open the About page
3) Observe the header obstruction
4) Turn Dark Mode on and then turn it off
5) Watch the change in the header as shown in the screenshots below

Expected Result: The header should be clear and unobstructed and upon turning off Dark Mode, the headers would return the colour it was in before turning on Dark Mode.

No Terminal Error Message.


Deakin Detonator Toolkit
Home
Dark mode
About
Attack Vectors
Tools
Walkthroughs
References
About The Toolkit


Deakin Detonator Toolkit
Home
Dark mode
About
Attack Vectors
Tools
Walkthroughs
References
About The Toolkit


Deakin Detonator Toolkit
Home
Dark mode
About
Attack Vectors
Tools
Walkthroughs
References
About The Toolkit