**GÖREV TANIMI:**

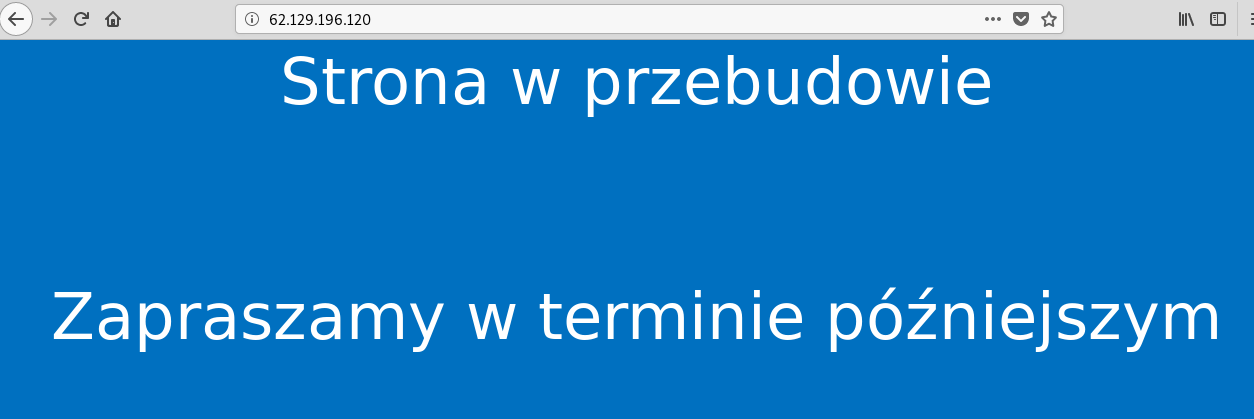
[**62.129.196.120**](http://62.129.196.120/)[**77.247.228.43**](http://77.247.228.43/)[**90.206.188.236**](http://90.206.188.236/)[**213.184.24.4**](http://213.184.24.4/)[**62.210.219.122**](http://62.210.219.122/)

**bu hedefler hakkında olabildiğince bilgi toplayın IP nerede, kime ait, ne işe yarıyor sunucu, hangi portları açık, neden açık, hangi servisler çalışıyor o portlarda, bu servislerin configürasyonları nasıl yapılmış, bu servislerden sistem hakknda ne tarz bilgiler elde ederiz**

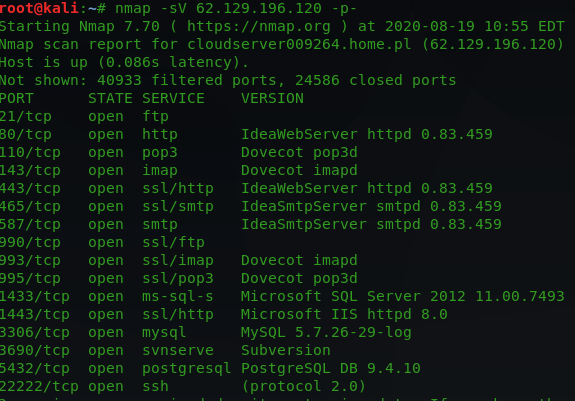
**Bu servis ve konfigürasyonlar hangi zafiyetleri taşıyor**

**HEDEF IP ADRESİ: 62.129.196.120**

**SİTE GÖRÜNÜMÜ:**



**NMAP AÇIK SERVİS TARAMASI:**



**\*\*Service Info: OS: Windows; CPE: cpe:/o:microsoft:Windows\*\***

**IP hangi ülkeye ait:Polonya**

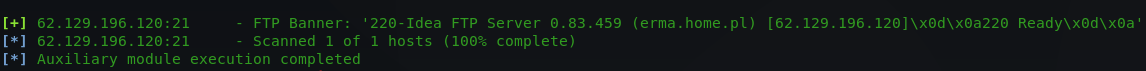
**Kime ait: RIPE Network Coordination Centre**

**Sunucu ne işe yarıyor :Sunucu bir Cloud Server**

**21.PORT**

21.portta FTP servisi çalışıyor ve biz bu servise anonymous olarak bağlanmayı başarabildik.

Daha sonra banner bilgisini almak için auxiliary(scanner/ftp/ftp\_version) modülünü kullandık burdan banner bilgisini okuyabiliyoruz.



**80.PORT**

80.Portta http servisinin çalıştığınızı görüyoruz. Versiyon olarak Idea Web Server kullanılmış.Gerekli zafiyet taramalarını yaptım fakat bi şey bulamadım.



**110.PORT**

110.Portta bir Pop3 servisi çalışıyor.Pop3 servisi bir mail servisidir. Başlık ve içeriğin birlikte olacak şekilde elektronik posta (e-posta, email) almak (posta kutusundaki mailleri çekmek) için kullanılır.Bu servisle ilgili bir zafiyet aradığımda şu iki zafiyetin olabileceğini buldum

* Seattle Lab Mail 5.5 [CVE-2003-0264]
  + MSF: exploit/windows/pop3/seattlelab\_pass
  + Exploit-DB: 638.py, 643.c, 646.c
* Cyrus – Gentoo 2006.0 Linux 2.6 [CVE-2006-2502]
  + MSF: exploit/linux/pop3/cyrus\_pop3d\_popsubfolders

Fakat metasploit üzerinden bu zafiyetlere exploit uyguladığımda bir sonuç elde edemedim

**143.PORT**

143.porttaa çalışan imap servisi (İnternet Mesaj Erişim Protokolü) kısaltmasıdır. IMAP size e-posta iletilerinizi doğrudan e-posta sunucusu üzerinde yönetme olanağı sunar.Imap için zafiyet taraması yaptık fakat zafiyet olmadığını gördük

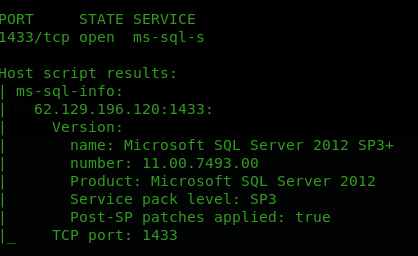
**587.PORT**

587.porta bir smtp servisi çalışıyor.Smtp bir mail protokolüdür. Smtp servisi ile ilgili bilgi toplarken banner bilgisine metasploit kullanarak ulaştım.

.

**1433.PORT**

Mssql servisinin çalıştığını gördüm ve buna ilişkin bilgiler topladım. Çalışan sürüm **Microsoft SQL Server 2012**



**3690.PORT**

Subversion sistemi bir dizi katmanlardan oluşmuş istemci-sunucu uygulamasıdır. **svnserve**yazılımı bu sistemin sunucusu olarak görev yapar. **svnserve**istemcilerden gelen isteklerini yerine getir.

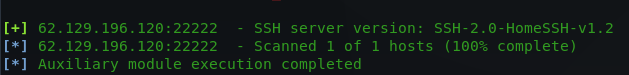
Eğer **bir brute force atağı yapılırsa buffer overflow** yapılabilir ve sunucunun yanıt verememesi gerçekleştirilebilir. Bundan yararlanarakta sistem sömürülebilir.

**5432.PORT**

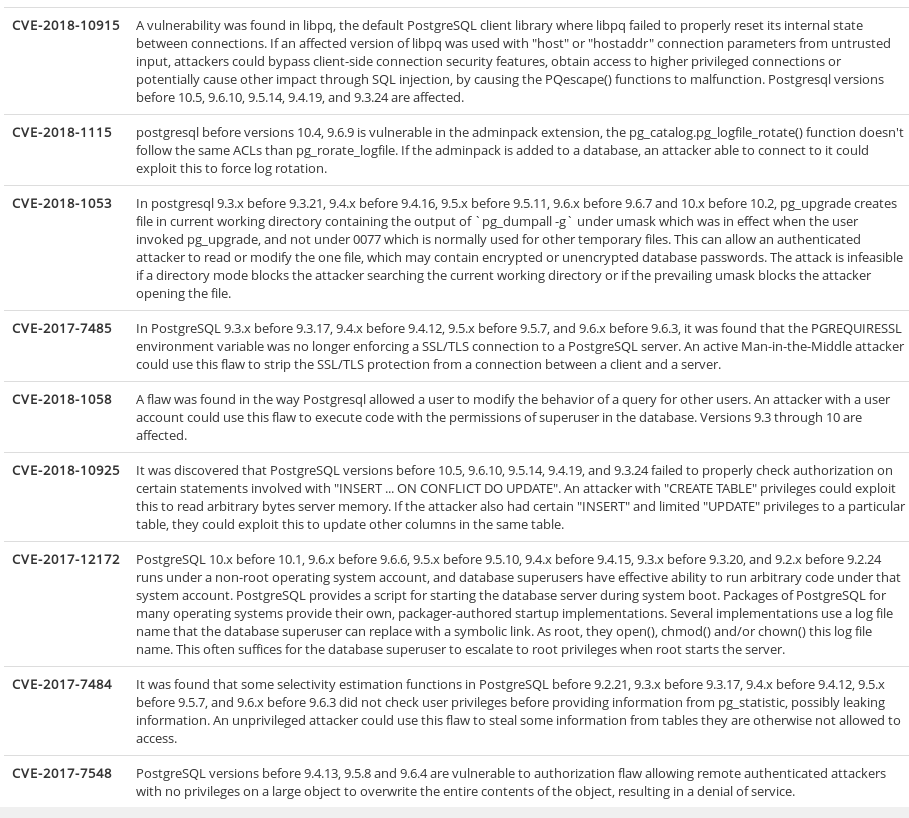
[**PostgreSQL**](https://wmaraci.com/nedir/postgresql), açık kaynaklı ve tamamen ücretsiz nesne ilişkisel veri tabanı sistemidir.Sürüm olarak 9.4.10 yı görüyoruz. Bu sürüme ait bir zafiyet bulamadım.

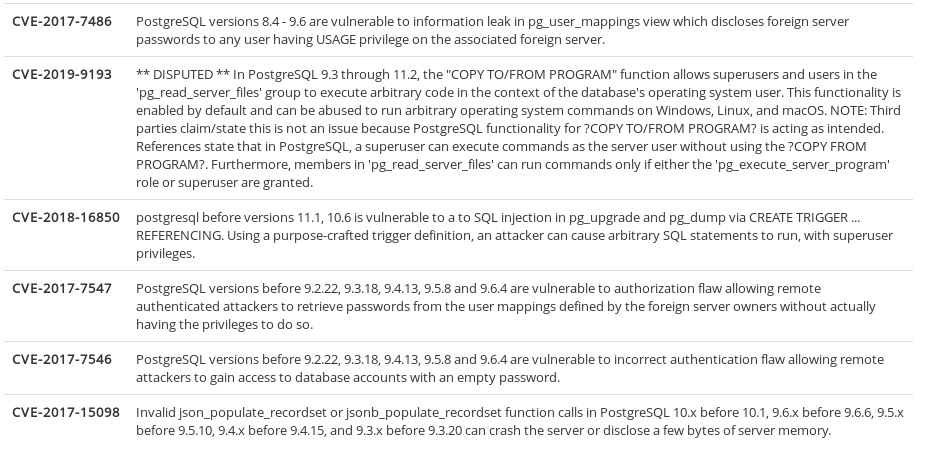
**22222.PORT**

Bu portta bir SSH servisi çalışığını görüyoruz. Sürüm bilgisini aşağıdaki gibi elde ettim



**BU IP ADRESİ ÜZERİNDE OLABİLECEK ZAFİYETLER LİSTESİ:**



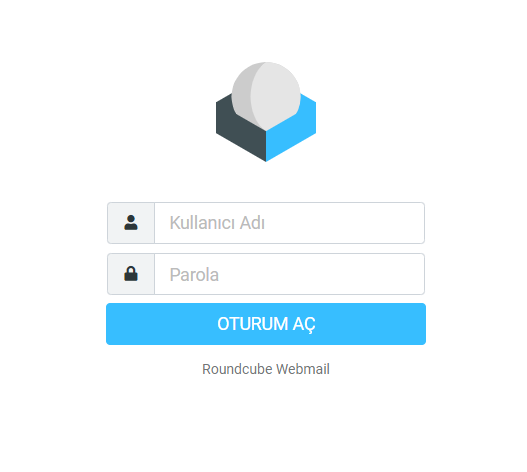


**WEB SİTESİNDE KULLANILAN TEKNOLOJİLER:**

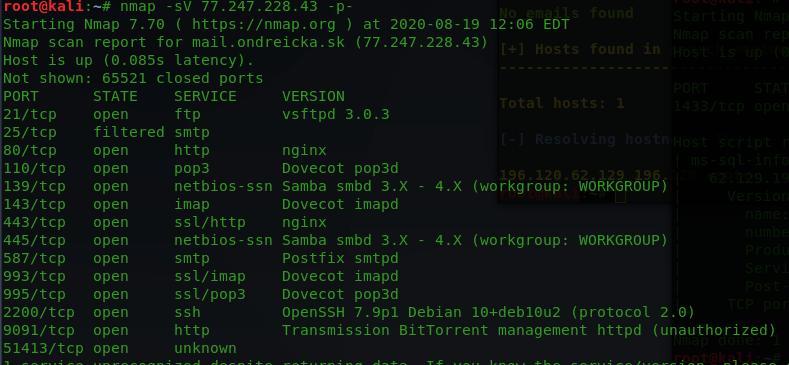


**HEDEF IP ADRESİ:77.247.228.43**

**SİTE GÖRÜNÜMÜ:**



**NMAP AÇIK SERVİS TARAMASI:**



**--Service Info: Hosts: MAIL, mail.ondreicka.sk; OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel—**

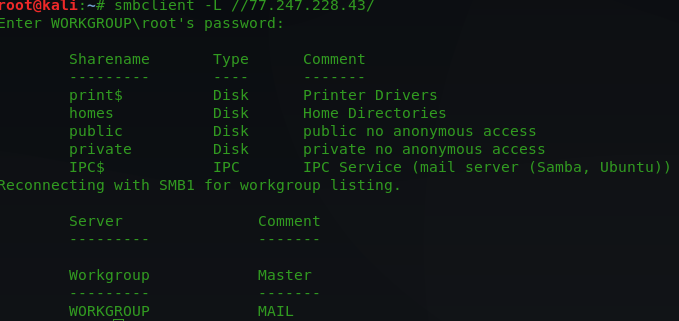
**IP hangi ülkeye ait:** **Slovakia**

**Kime ait: ISPER, s.r.o.**

**Sunucu ne işe yarıyor :Sunucu bir Mail Servisi**

**21.PORT**

21. Portta çalışan bir ftp vsftpd 3.0.3 protokolünü gördük ve **anonymous olarak bağlanmayı server reddetmektedir.** .Ftp protokolü bir dosya transfer protokolüdür.



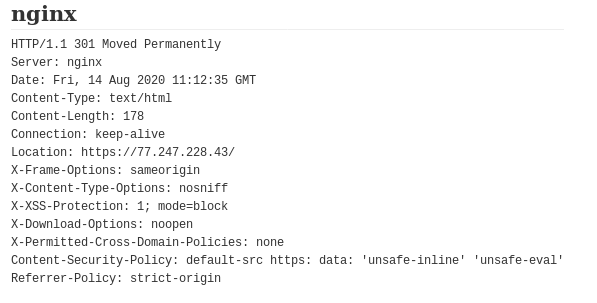
Burdan bir bilgi elde edemedik ve yaptığımız araştırmalardan da vsftpd 3.0.3 ında bilinen bir zafiyeti olmadığını gördük.Fakat dosyaları görüntülemiş olduk

**80.PORT**

80. portta çalışan http servisini ve versiyon olarak da nginx kullandığını gördük. [**Nginx**](https://www.nginx.com/) bir mail sunucusudur.

Nginx için metasploitte bir zafiyet aradık.

nginx - Cannot exploit: the remote server is not vulnerable - Version nginx Fakat ngix in bu versiyonda bir zafiyeti olmadığını gördük.



Header başlığında 301 Moved Permanently diyor ve portlara bakınca ssl/http görüyoruz.Yani http den https ‘e bir yönlendirme yapılmış.

**110.PORT**

110. portta çalışan pop3 servisi versiyon olarak Dovecot pop3d. **Dovecot**  kullanıcıların ağdaki posta aktarımlarını **pop3** veya imap protokollerini kullanarak göndermesini sağlayan açık kaynak kodlu bir yazılımdır. Pop3 için zafiyet taraması yaptık fakat zafiyet olmadığını gördük.

**139.PORT**

139. portta çalışan samba servisin zafiyet taramalarını gerçekleştirdik fakat bir zafiyete rastlanmadı.

**143.PORT**

143.porttaa çalışan imap servisi (İnternet Mesaj Erişim Protokolü) kısaltmasıdır. IMAP size e-posta iletilerinizi doğrudan e-posta sunucusu üzerinde yönetme olanağı sunar.Imap için zafiyet taraması yaptık fakat zafiyet olmadığını gördük.

**443.PORT**

443. portta çalışan ssl/http servisini ve versiyon olarak da nginx kullandığını gördük. [**Nginx**](https://www.nginx.com/) bir mail sunucusudur.

Nginx için metasploitte bir zafiyet aradık.

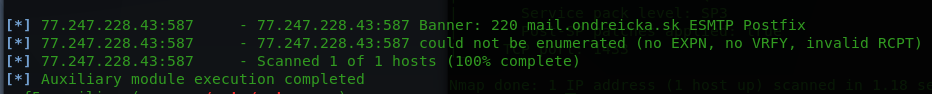
nginx **- Cannot exploit: the remote server is not vulnerable - Version nginx** Fakat ngix in bu versiyonda bir zafiyeti olmadığını gördük.

**445.PORT**

445. portta çalışan samba servisin zafiyet taramalarını gerçekleştirdik fakat bir zafiyete rastlanmadı.

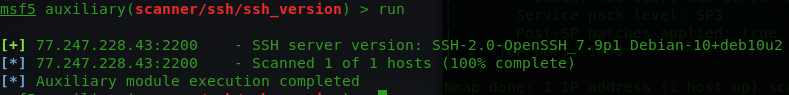
**587.PORT**

587. porta bir smtp servisi çalışıyor .Smtp bir mail protokolüdür.Banner bilgisene ulaştım:

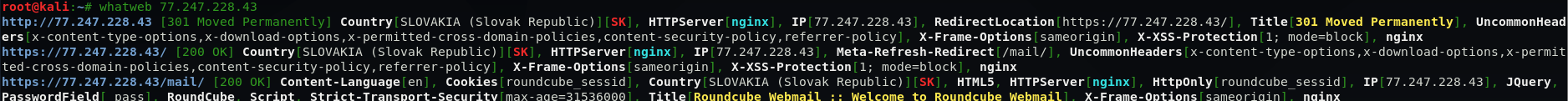


**2200.PORT**

Bu portta bir SSH servisi çalışığını görüyoruz. Banner bilgisini aşağıdaki gibi elde ettim



**77.247.228.43 ip adresini whatweb ile header bloğunu çektiğimizde dikkatimi çeken X-XSS-Protection: 1; mode=block olmuştu bunun bir mail sitesi olmasından ve bir login girişi olduğundan dolayı xss payloadlarını bloke etmesi dikkatimi çekti.**

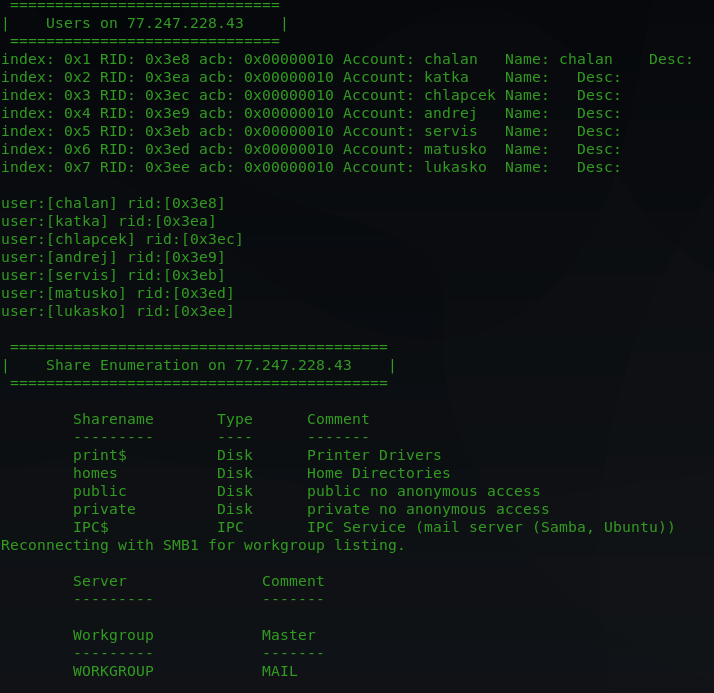


X-XSS-Protection: 1; mode=block

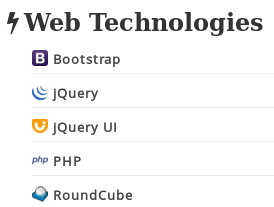
Tarayıcıda XSS güvenlik filtresini devreye alır. Olası bir XSS payloadunun sayfada çalışmasını tüm sayfanın gösterilmesini engelleyerek bloke eder. XSS payloadu gönderildiğinde, ziyaretçi browserda beyaz bir ekran ile karşılaşır.

Enum4linux komutu ile bazı **account bilgilerine** ulaştık.

**enum4linux -U -o 77.247.228.43**

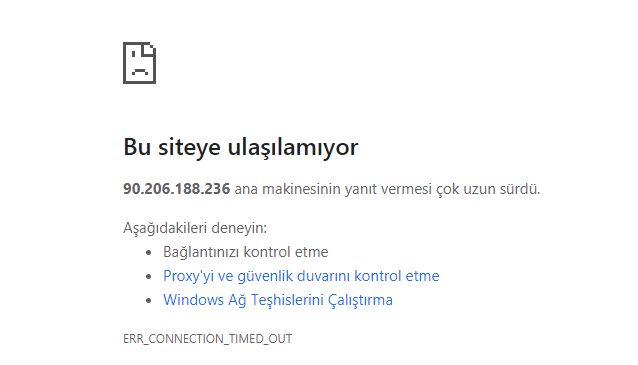


**WEB SİTESİNDE KULLANILAN TEKNOLOJİLER:**

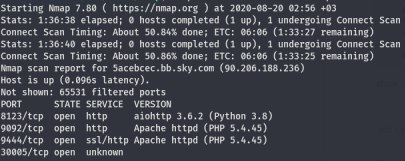


**HEDEF IP ADRESİ: 90.206.188.236**

**SİTE GÖRÜNÜMÜ:Connection timed-out hatası aldım**



**NMAP AÇIK SERVİS TARAMASI:**



Shodan.io kullanarak IP adresine ait servisler hakkımda ayrıntılı bilgiler elde ettim.













**IP hangi ülkeye ait: United Kingdom**

**Kime ait: Sky Broadband**

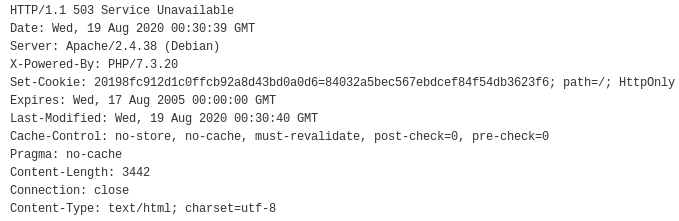
**22.PORT**

22. port üzerinde çalışan bir ssh servisi var ve bu ssh servisinin versiyon bilgisi:

**SSH-2.0-OpenSSH\_8.2p1 Ubuntu-4ubuntu0.1**

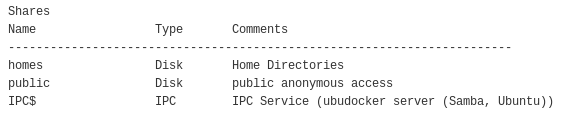
**80.PORT**

**Bu portta bir Apache servisi çalışmaktadır. Header bilgisi:**

Header bilgisinde 503 yani Servise ulaşılamıyor şeklinde bir bilgi gördüm.Bu da hosting firmasından kaynaklanıyormuş

**445.PORT**

Bu portta Smb protokolü çalışıyor.Klasörleri bu şekilde listeledim :



**3306.PORT**

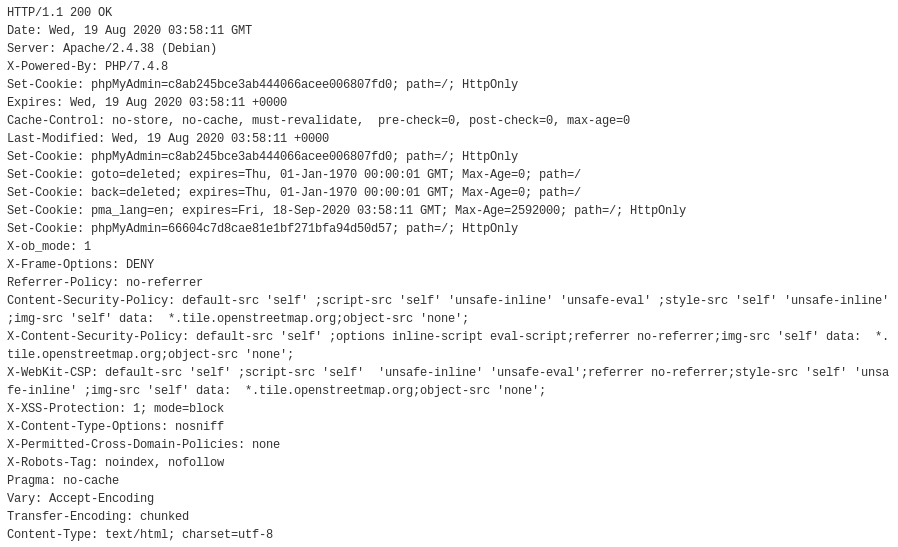
Bu portta bir mysql veritabanı çalıştığını gördüm.Veritabanı versiyon bilgisi:

**Version: 5.5.5-10.5.2-MariaDB-1**

Bir zafiyet araştırdım fakat bulamadım.

**8081.PORT**

Apache sunucusu çalışmakta. Header bilgisi:

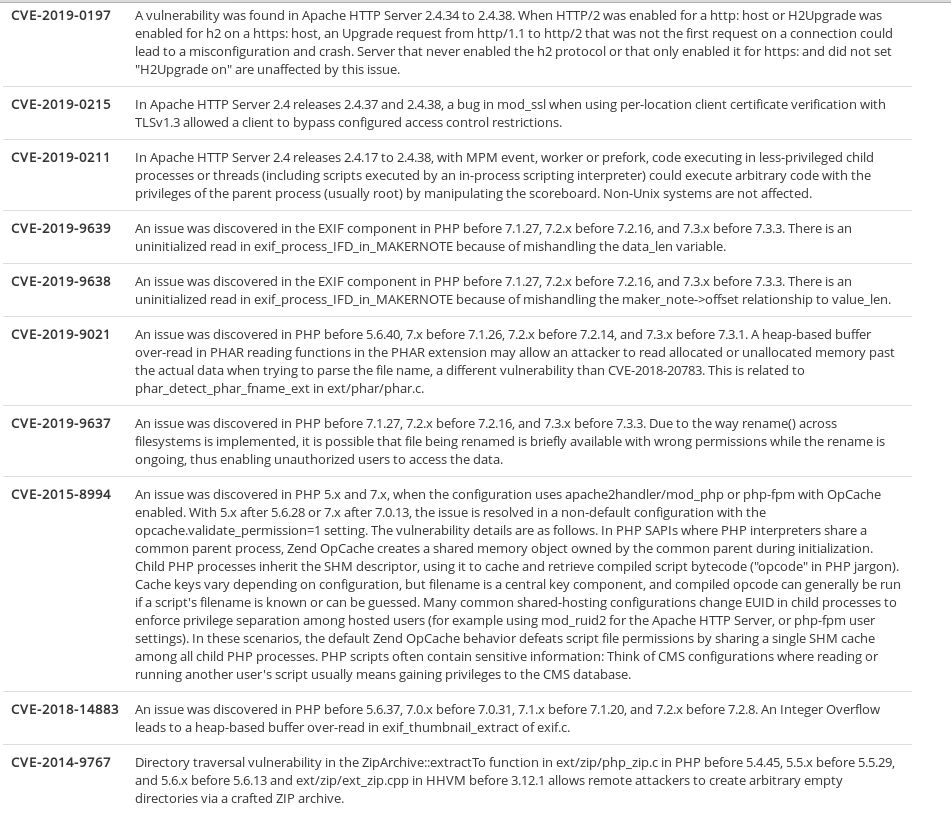


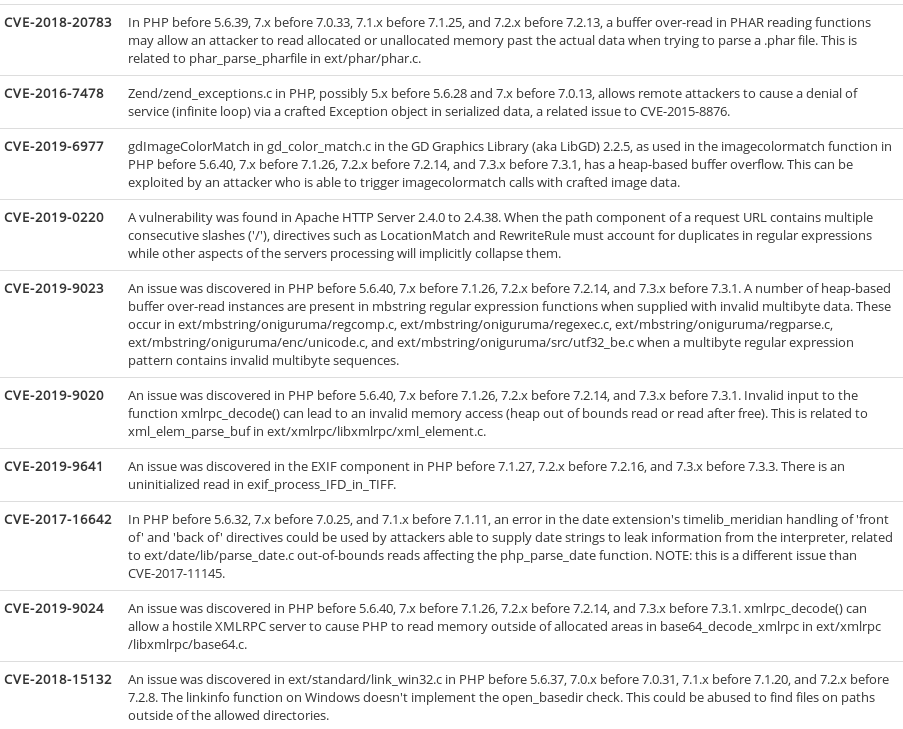
**8123.PORT**

Bu port üzerinde çalışan aiohttp servisi pythonda bir Asynchronous programlama türüdür.Asynchronous programlama demek aslında teknik olarak tek bir thread üzerindeki bir event loop üzerinde çalışan async-aware metotların görev değişimi yapmaları demekmiş.Bu porttan bir zafiyet bulamadım

**BU IP ADRESİ ÜZERİNDE OLABİLECEK ZAFİYETLER LİSTESİ:**





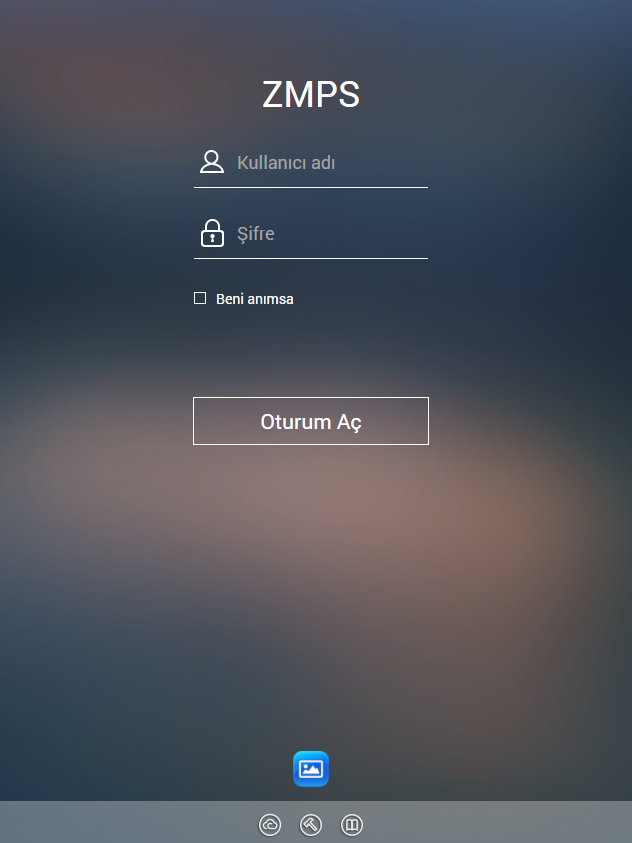


**WEB SİTESİNDE KULLANILAN TEKNOLOJİLER:**

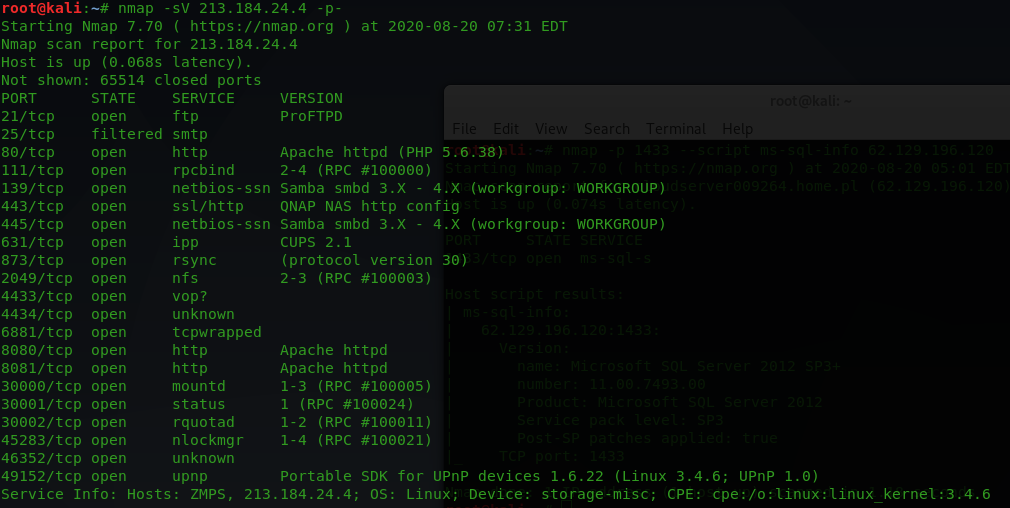


**HEDEF IP ADRESİ: 213.184.24.4**

**SİTE GÖRÜNÜMÜ:**



**NMAP AÇIK SERVİS TARAMASI:**



**\*\* Service Info: Hosts: ZMPS, 213.184.24.4; OS: Linux; Device: storage-misc; CPE: cpe:/o:linux:linux\_kernel:3.4.6\*\***

## \*\*Linux kernel :3.4.6 için exploit araştırması yaptığımda CVE-2016-10229 kodlu bir zafiyetin bulunduğunu gördüm. \*\*

**IP hangi ülkeye ait:Polonya**

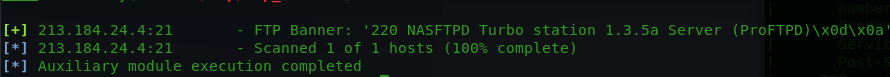
**Kime ait: University of Warmia and Mazury in Olsztyn, Poland**

**Sunucu ne işe yarıyor :Sunucu bir Cloud Server**

**21.PORT**

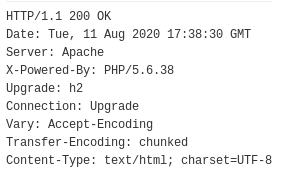
21.portta FTP servisi çalışıyor ve biz bu servise **anonymous** olarak bağlanmayı denedik fakat sistem tarafından anonymous olarak bağlantı gerçekleştiremedik

Daha sonra banner bilgisini almak için auxiliary(scanner/ftp/ftp\_version) modülünü kullandım burdan banner bilgisini okuyabiliyoruz.



**80.PORT**

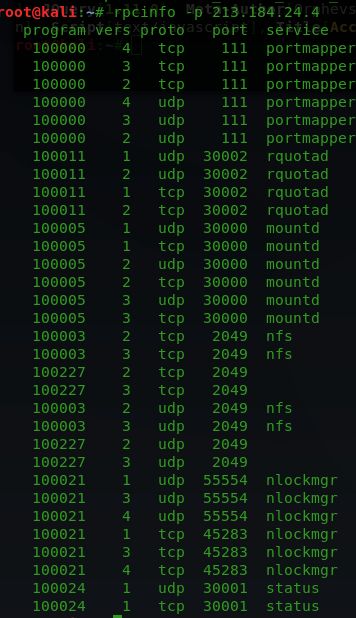
80.porrta bir apache servisi mevcur.Header bilgisi aşağıdaki gibi:

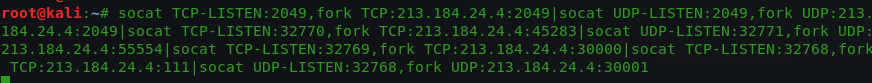


**111.PORT**

111.portta rpcbind, çalışan RPC hizmetlerinin sayısına bağlı olarak x5 ve x20 arasında bir yükseltme faktörüne sahip olabilir. Herkese açık olarak açıklanmamalı veya en azından yalnızca beyaz listeye alınmış IP adreslerine izin verilmemelidir, aksi takdirde sunucuyu DDoS saldırılarına katıldığını görebilirsiniz.

rpcinfo -p 2013.184.24.4





RPC servisleri listeledikten sonra portlaro socat ile dinlemeye aldım fakat daha sonrasında çalıştırdığım komut:



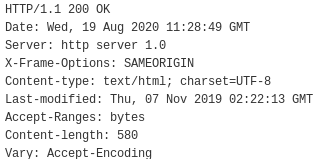
Çalışmadı ve ilerleme kaydedemedim. Bu hatanın çözümü nfs sistemini tekrardan başlatmakmış.

**139.PORT**

139. portta çalışan samba servisin zafiyet taramalarını gerçekleştirdik fakat bir zafiyete rastlanmadı.

**443.PORT**

443.portta çalışan ssl/http servisinin header başlığı:



**Ayrıca sürüm olarak QNAP NAS kullanılmakta**

**QNAS NAS** Ağa Bağlı Depolama (NAS) cihazı, verilerin yetkili kullanıcılar ve farklı müşteriler için merkezi bir konumda depolanmasını ve buradan güvenle paylaşılmasını sağlayan ağa bağlı bir depolama cihazıdır.

**631.PORT**

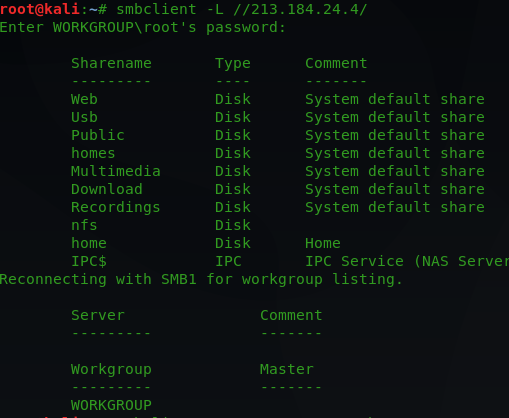
631.Portta IPP protokolünü görüyoruz ve versiyon olaran CUPS 2.1. CUPS yazdırma işlerini ve kuyruklarını yönetir ve yazıcılar çok geniş bir ürün yelpazesi için destek sunarken lazer ve aralarında birçok nokta-matris, standart Internet Yazdırma Protokolü’nü (IPP) kullanarak ağ üzerinden yazdırma sağlar. CUPS da PostScript Yazıcı Tanımı (PPD) ve ağ yazıcıları otomatik algılama destekler ve basit bir web tabanlı konfigürasyon ve yönetim aracı bulunmaktadır.

**6881.PORT**

6881.portta bir tcpwapper isimli servis çalıştığını gördük.Bu servis bir firewall gibi çalışıp ağ erişimini filtrelemek için kullanılır**.**TCP Wrapper, Linux veya BSD olarak işletim sistemleri üzerinde Internet Protokolü sunucularına ağ erişimini filtrelemek için kullanılan bir barındırma-tabanlı ağ erişim denetim listesi.

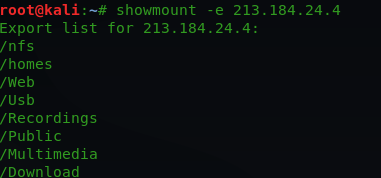
**445.PORT**

445. portta çalışan samba servisin zafiyet taramalarını gerçekleştirdik fakat bir zafiyete rastlanmadı. Fakat aşağıdaki klasör isimlerini çekebildim.

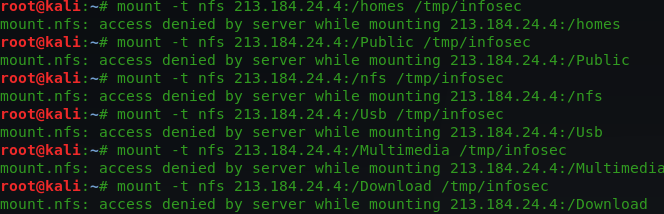


**2049.PORT**

**2049.portta NFS(Network File System) servisini görüyoruz.** ,NFS **linux** sistemler arasında dosya paylaşamını sağlayan ve stabil çalışan bir teknolojidir. NFS servisindeki dosyaları bu şekilde listeledik.



Daha sonra dosyalara erişimimiz olup olmadığı kontrol ettim



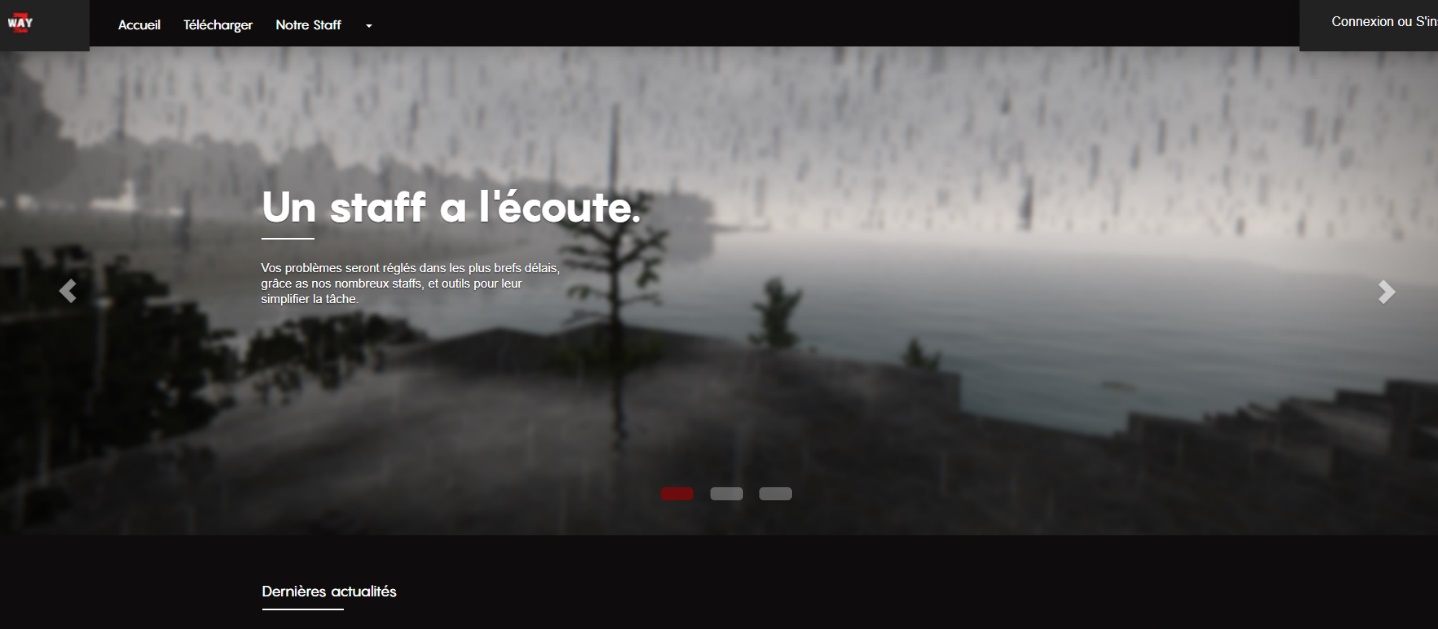
Erişimiz olmadığını gördüm.

**BU IP ADRESİ ÜZERİNDE OLABİLECEK ZAFİYETLER LİSTESİ:**

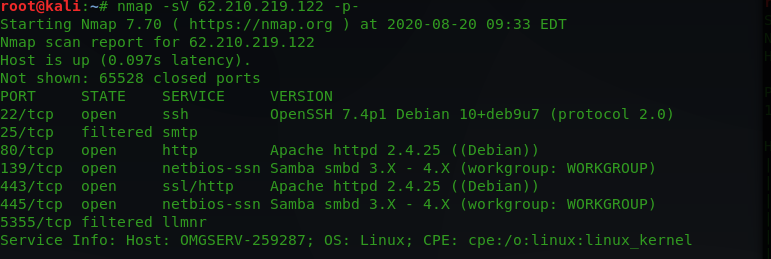


**HEDEF IP ADRESİ: 62.210.219.122**

**SİTE GÖRÜNÜMÜ:**



**NMAP AÇIK SERVİS TARAMASI:**



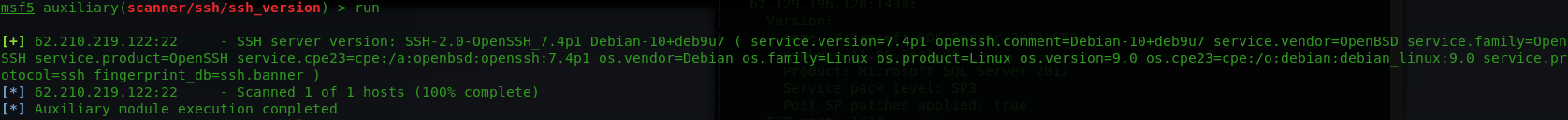
**\*\*Service Info: Host: OMGSERV-259287; OS: Linux; CPE: cpe:/o:linux:linux\_kernel\*\***

**IP hangi ülkeye ait:** **France**

**Kime ait: Dedibox SAS**

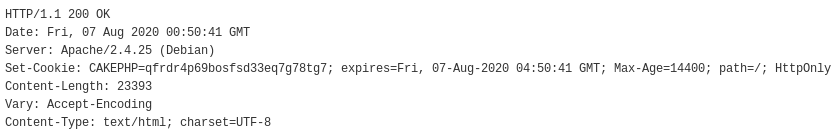
**22.PORT**

Bu portta bir SSH servisi çalışığını görüyoruz. Banner bilgisini aşağıdaki gibi elde ettim



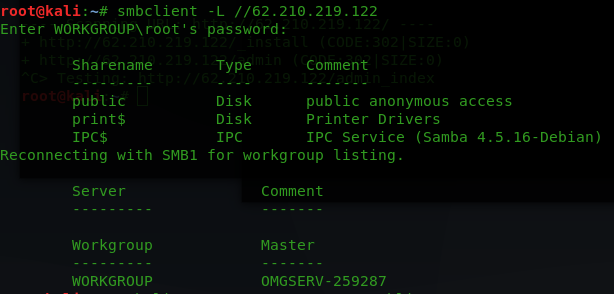
**80.PORT**

80.portta bir Apache servisi çalışıyor. Bu Apache servisinin header bilgisi:

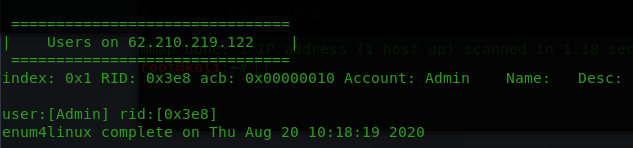


**445.PORT**

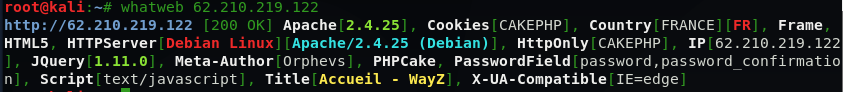
Bu portta smblient ile dosyaları aşağıdaki gibi listeledim:



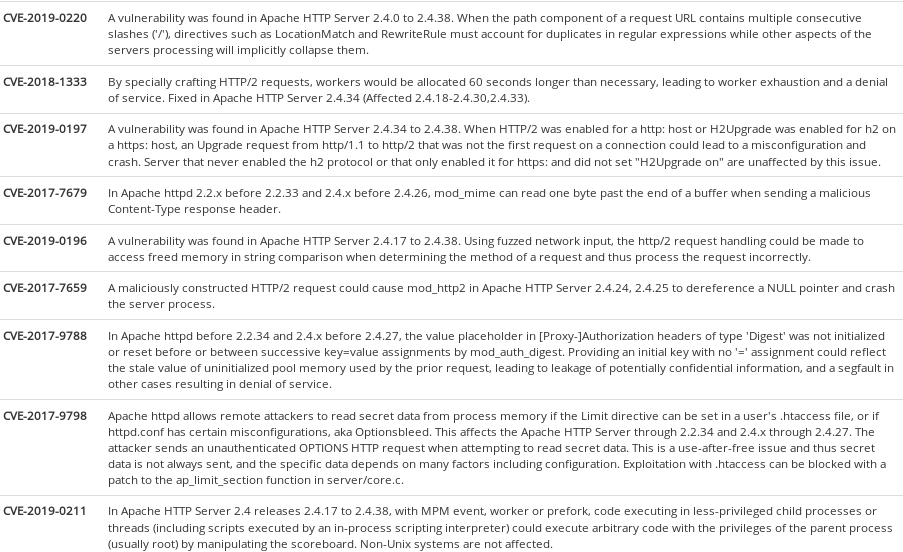
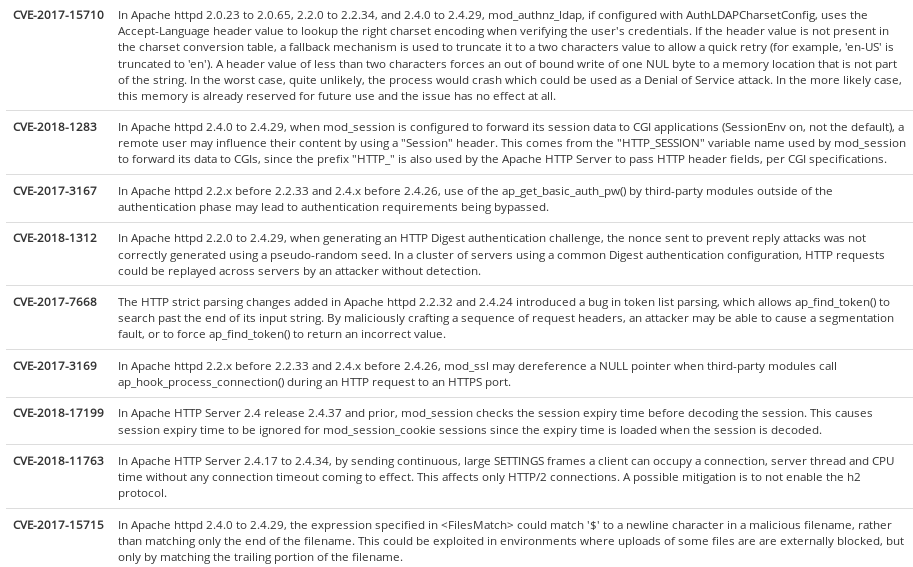
Enum4linux ile Admin isimli bir hesap olduğunu buldum.



**Whatweb kullanarak web sitesi hakkında bilgiler edindim:**



**BU IP ADRESİ ÜZERİNDE OLABİLECEK ZAFİYETLER LİSTESİ:**



**WEB SİTESİNDE KULLANILAN TEKNOLOJİLER:**

