

Experiment-09: File Inclusion Vulnerabilities

Go to file inclusion tab



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



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



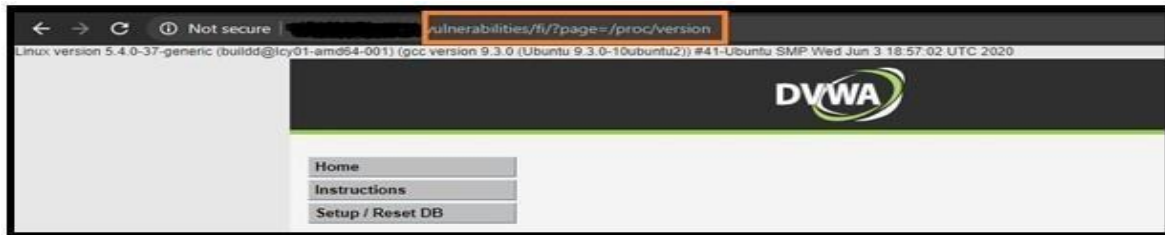
File Inclusion Source (Security Level: MEDIUM)



Change include.php to /etc/passwd



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



Security Level: HIGH

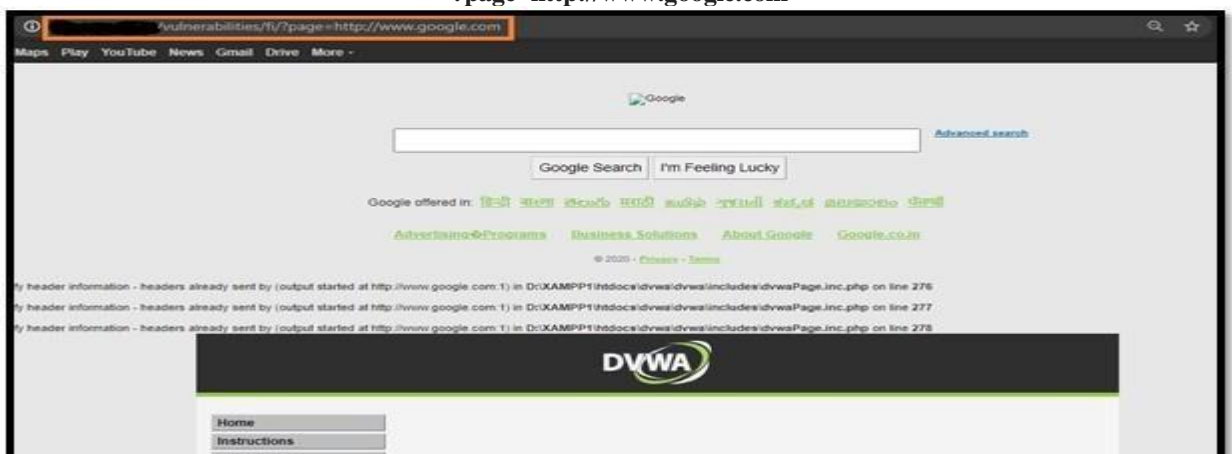
Change the URL from `include.php` to `?page=file:///etc/passwd`, You will get the data of `/etc/passwd` file.



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`



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

