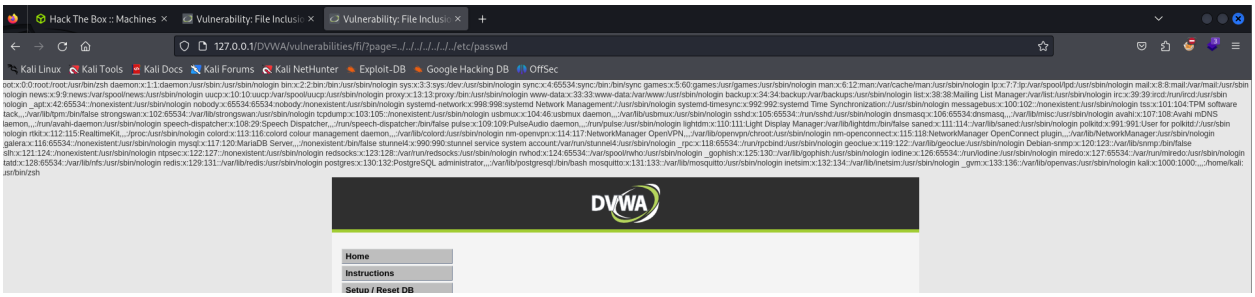
File Inclusion

- LFI stands for **Local File Includes** - it's a file local inclusion vulnerability that allows an attacker to include files that exist on the target web server
- Typically this is exploited by abusing dynamic file inclusion mechanisms that don't sanitize user input
- Found some interesting on LFI Cheat Sheet

1. **Low**

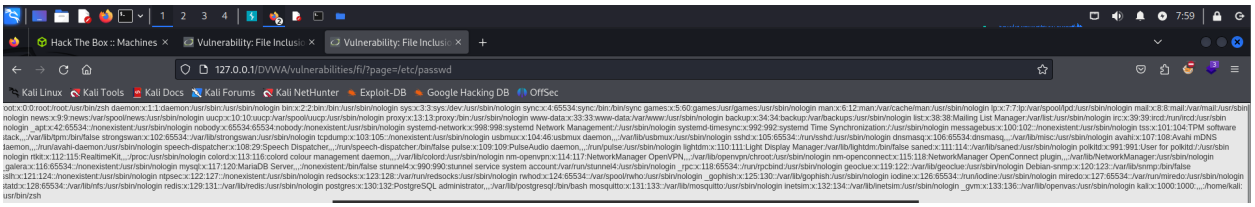
- Let's try with the directory traversal payload

```
foo.php?file=../../../../../../../etc/passwd
```



2. **Medium**

- Seeing the src code, it have parametered to remove the "http://", "https://" and "../" và "..\" so we can't path travelsal
- Trying `/etc/passwd` and get the result



- Also worked with `/bin/bash`

3. **High**

- In this level, I tried the same method in medium level but it seems didn't working
- The source code told me that it will only work when it start with value `file` or `include.php`
- After some research, I found the `:///` indicating that this is an absolute path from the root of the file system
- `file` indicating that this URL can access to the file system