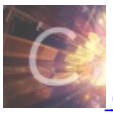
[wargame.kr 韩国 CTF] Writeup

原创

你们这样一点都不可耐 于 2020-08-07 09:00:19 发布 121 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/vanarrow/article/details/107854361



[wargame.kr 韩国 CTF]

1.
2.
3.
4.

1.

2.

3.

4.

> 135point / bughela
> I have accounts. but, it's blocked.
> can you login bypass filtering?

```php
<?php

if (isset($_GET['view-source'])) {
    show_source(__FILE__);
    exit();
```

```
    exit();
}

/*
create table user(
 idx int auto_increment primary key,
 id char(32),
 ps char(32)
);
*/

 if(isset($_POST['id']) && isset($_POST['ps'])){
  include("../lib.php"); # include for auth_code function.

  mysql_connect("localhost","login_filtering","login_filtering_pz");
  mysql_select_db ("login_filtering");
  mysql_query("set names utf8");

  $key = auth_code("login filtering");

  $id = mysql_real_escape_string(trim($_POST['id']));
  $ps = mysql_real_escape_string(trim($_POST['ps']));

  $row=mysql_fetch_array(mysql_query("select * from user where id='$id' and ps=md5('$ps')"));

  if(isset($row['id'])){
   if($id=='guest' || $id=='blueh4g'){
    echo "your account is blocked";
   }else{
    echo "login ok"."<br />";
    echo "Password : ".$key;
   }
  }else{
   echo "wrong..";
  }
 }
?>
<!DOCTYPE html>
<style>
 * {margin:0; padding:0;}
 body {background-color:#ddd;}
 #mdiv {width:200px; text-align:center; margin:50px auto;}
 input[type=text],input[type=[password] {width:100px;}
 td {text-align:center;}
</style>
<body>
<form method="post" action="./">
<div id="mdiv">
<table>
<tr><td>ID</td><td><input type="text" name="id" /></td></tr>
<tr><td>PW</td><td><input type="password" name="ps" /></td></tr>
<tr><td colspan="2"><input type="submit" value="login" /></td></tr>
</table>
 <div><a href='?view-source'>get source</a></div>
</form>
</div>
</body>
<!--

you have blocked accounts.
```

```
guest / guest
blueh4g / blueh4g1234ps

-->
```

```
<!--

you have blocked accounts.

guest / guest
blueh4g / blueh4g1234ps

-->
```

大小写绕过

```
比如
账户Guest
密码guest
或者

账户
blueh4G
密码
blueh4g1234ps
```

login ok
Password : 9909bc0d66546b9c85f28ce8589261bcff7fea15

ID
PW
login

get source