mysql溢出漏洞_Natas27 Writeup（mysql溢出截断漏洞）

原创

weixin_39792393 于 2021-01-28 05:17:25 发布 29 收藏
文章标签： mysql溢出漏洞

本文链接：https://blog.csdn.net/weixin_39792393/article/details/113460970

Natas27：

一个登录节界面，查看源码。

natas27

```
// morla / 10111

// database gets cleared every 5 min

/*

CREATE TABLE `users` (

`username` varchar(64) DEFAULT NULL,

`password` varchar(64) DEFAULT NULL //这是重点，用户名和密码均不超过64个字节

);

*/

function checkCredentials($link,$usr,$pass){

//转义用户名和密码中的特殊字符，防止sql注入

$user=mysql_real_escape_string($usr);

$password=mysql_real_escape_string($pass);

$query = "SELECT username from users where username='$user' and password='$password' ";

$res = mysql_query($query, $link);
```

```
if(mysql_num_rows($res) > 0){ //若查询出来的数组大于0，则验证用户名/密码成功
return True;
}
return False;
}
function validUser($link,$usr){
$user=mysql_real_escape_string($usr);
$query = "SELECT * from users where username='$user'";
$res = mysql_query($query, $link);
if($res) {
if(mysql_num_rows($res) > 0) {
return True;
}
}
return False;
}
function dumpData($link,$usr){
$user=mysql_real_escape_string($usr);
$query = "SELECT * from users where username='$user'";
$res = mysql_query($query, $link);
if($res) {
if(mysql_num_rows($res) > 0) {
while ($row = mysql_fetch_assoc($res)) { //mysqli_fetch_assoc() 函数从结果集中取得一行作为关联数组。
// thanks to Gobo for reporting this bug!
//return print_r($row);
return print_r($row,true);
}
}
}
return False;
}
```

```
function createUser($link, $usr, $pass){
$user=mysql_real_escape_string($usr);
$password=mysql_real_escape_string($pass);
$query = "INSERT INTO users (username,password) values ('$user','$password')";
$res = mysql_query($query, $link);
if(mysql_affected_rows() > 0){ //mysqli_affected_rows() 函数返回前一次 MySQL 操作所影响的记录行数
return True;
}
return False;
}
//逻辑：查询username是否存在
if(array_key_exists("username", $_REQUEST) and array_key_exists("password", $_REQUEST)) {
$link = mysql_connect('localhost', 'natas27', '');
mysql_select_db('natas27', $link); //mysql_select_db() 函数设置活动的 MySQL 数据库。
if(validUser($link,$_REQUEST["username"])) {
//user exists, check creds
if(checkCredentials($link,$_REQUEST["username"],$_REQUEST["password"])){
echo "Welcome " . htmlentities($_REQUEST["username"]) . "!
"; //htmlentities() 函数把字符转换为 HTML 实体。
echo "Here is your data:
";
$data=dumpData($link,$_REQUEST["username"]);
print htmlentities($data);
}
else{
echo "Wrong password for user: " . htmlentities($_REQUEST["username"]) . "
";
}
}
else {
//user doesn't exist
if(createUser($link,$_REQUEST["username"],$_REQUEST["password"])){
```

```
echo "User " . htmlentities($_REQUEST["username"]) . " was created!";

}

}

mysql_close($link);

} else {?>

Username:
Password:

}?>
```

View sourcecode