

# BUUCTF 加固题 Ezsqli wp

原创

[whathay](#) 于 2022-02-04 15:35:28 发布 2835 收藏

分类专栏: [buuctf](#) 文章标签: [php](#) [mysql](#) [安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: [https://blog.csdn.net/weixin\\_52829570/article/details/122783579](https://blog.csdn.net/weixin_52829570/article/details/122783579)

版权



[buuctf](#) 专栏收录该内容

1 篇文章 0 订阅

订阅专栏

题目:

题目

解题快手榜

×

## Ezsqli

### 1

靶机地址解释: 第一行: 目标机器 WEB 服务地址第二行: 目标机器 SSH 地址以及端口第三行: Check 服务访问地址

修复方法:

1. SSH 连接上目标机器, 用户 ctf, 密码 123456。
2. 对目标机器上的服务进行加固。
3. 访问 Check 服务的 /check 进行 check。
4. 若返回 True, 则访问 /flag 可获得 /flag。
5. 每次 check 后目标机器会重置。

#### 一. 漏洞

在登录页面存在 sql 注入, 可用万能密码进行登录

我还可以教你，敦 dua 郎哦。

## 让我访问

用户名

密码

提交

登录成功!

用户名: admin' or 1=1#

密码: 随便

这道题就是加固这个登录页面的sql注入即可获取flag

### 二. 加固

根据给的地址和端口ssh连接目标机器，进入/var/www/html目录

在此处新建一个phpinfo.php并写入语句<?php phpinfo(); ?>

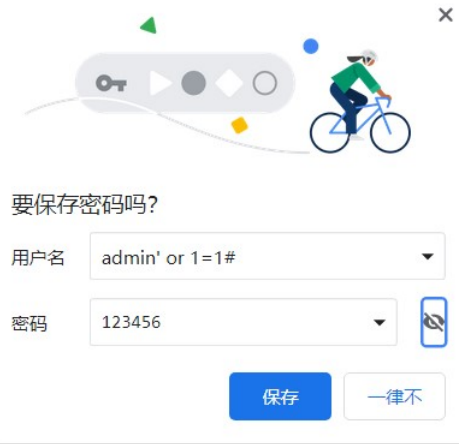
访问phpinfo.php可以看到当前php版本为7.3.18

PHP Version 7.3.18



System	Linux web2 4.19.221-0419221-generic #202112141049 SMP Tue Dec 14 11:54:51 UTC 2021 x86_64
Build Date	May 15 2020 13:24:46
Configure Command	./configure '--build=x86_64-linux-gnu' '--with-config-file-path=/usr/local/etc/php' '--with-config-file-scan-dir=/usr/local/etc/php/conf.d' '--enable-option-checking=fatal' '--with-mhash' '--enable-ftp' '--enable-mbstring' '--enable-mysqlnd' '--with-password-argon2' '--with-sodium=shared' '--with-pdo-sqlite=/usr' '--with-sqlite3=/usr' '--with-curl' '--with-libedit' '--with-openssl' '--with-zlib' '--with-libdir=lib/x86_64-linux-gnu' '--with-apxs2' '--disable-cgi' 'build_alias=x86_64-linux-gnu'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc/php

php中防止sql注入的函数无非就那么几个(我所知道的)



addslashes()

mysql\_real\_escape\_string() 在php5.5中已经弃用，并在php7中被删除

mysql\_escape\_string() PHP 4 >= 4.0.3, PHP 5

很明显这三个在php7中只有addslashes()还能使用

所以在index.php中添加如下代码

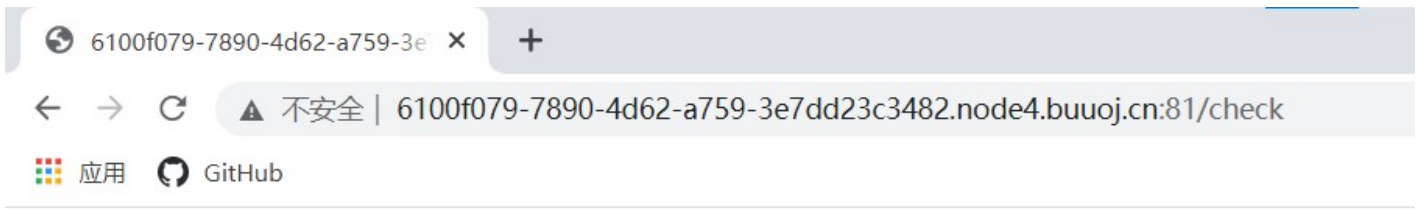
```
$username = addslashes($username);  
$password = addslashes($password);
```

修改后的文件

```
1 buu_index.php x  
190 </div>  
191 </body>  
192 </html>  
193 <h4 style="text-align: center; color: #000000">  
194 <?php  
195 error_reporting(0);  
196 include 'dbConnect.php';  
197 $username = $_GET['username'];  
198 $password = $_GET['password'];  
199  
200 //在预定义字符之前添加反斜杠,预定义字符:单双引号,反斜杠等  
201 $username = addslashes($username);  
202 $password = addslashes($password);  
203  
204  
205 if (isset($_GET['username']) && isset($_GET['password'])) {  
206     $sql = "SELECT * FROM users WHERE username = '$username' AND password = '$password'";  
207     $result = $mysqli->query($sql);  
208     if (!$result)  
209         die(mysqli_error($mysqli));  
210     $data = $result->fetch_all(); // 从结果集中获取所有数据  
211     if (!empty($data)) {  
212         echo '登录成功;!  
213     } else {  
214         echo "用户名或密码错误"  
215     }  
216 }  
217 ?>  
218 </h4>
```

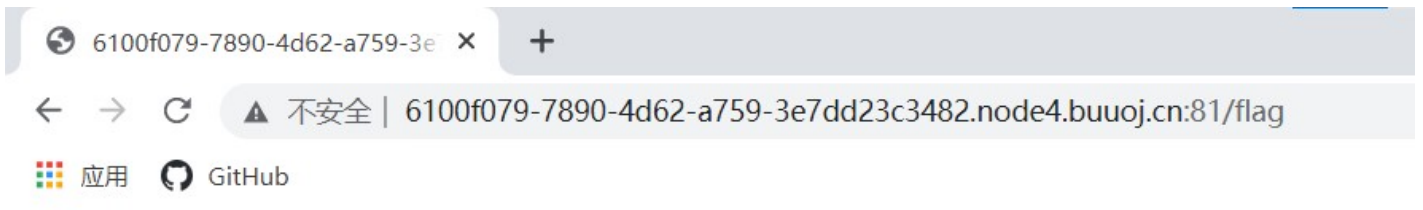
### 三. 拿flag

访问 Check 服务的 /check进行 check



Please wait 60s... Checking in progress...

然后访问/flag即可拿到flag



Your flag: flag{85a6edf4-fac5-47b7-bc21-e79e62e7f102}



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)