BUUCTF 加固题 Ezsql wp

原创

whathay 于 2022-02-04 15:35:28 发布
分类专栏： buuctf 文章标签： php mysql 安全

题目：

一. 漏洞

在登录页面存在sql注入,可用万能密码进行登录

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

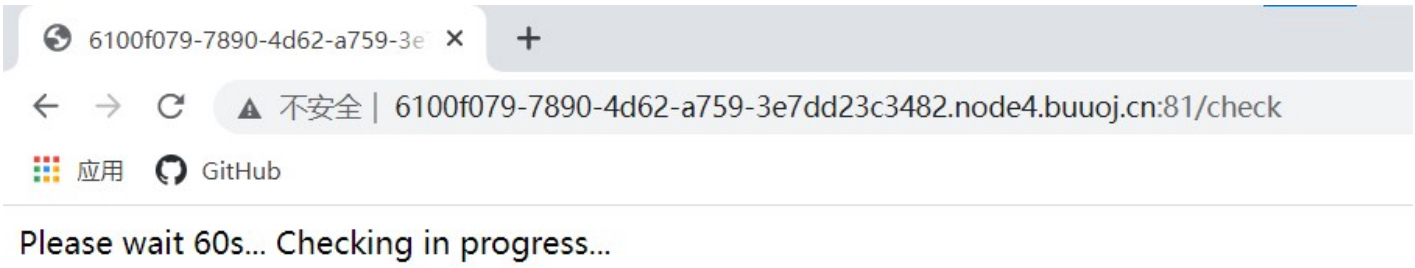
```
</div>
</body>
</html>
<h4 style="text-align: center; color: #000000">
<?php
error_reporting(0);
include 'dbConnect.php';
$username = $_GET['username'];
$password = $_GET['password'];

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


if (isset($_GET['username']) && isset($_GET['password'])) {
    $sql = "SELECT * FROM users WHERE username = '$username' AND password = '$password'";
    $result = $mysqli->query($sql);
    if (!$result)
        die(mysqli_error($mysqli));
    $data = $result->fetch_all(); // 从结果集中获取所有数据
    if (!empty($data)) {
        echo '登录成功！'
    } else {
        echo "用户名或密码错误"
    }
}
?>
</h4>
```

三. 拿flag

访问 Check 服务的 /check进行 check



然后访问/flag即可拿到flag