




BUUCTF加固题 Ezsql

原创

静默开水  于 2022-02-14 14:44:16 发布  2731  收藏

分类专栏: [BUU题解](#) [漏洞加固](#) [CTF](#) 文章标签: [web安全](#) [安全](#) [经验分享](#) [安全漏洞](#)

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/cadandme/article/details/122923056>

版权



[BUU题解](#) 同时被 3 个专栏收录

3 篇文章 0 订阅

订阅专栏



[漏洞加固](#)

1 篇文章 0 订阅

订阅专栏



[CTF](#)

14 篇文章 0 订阅

订阅专栏

题目重新复现

- 在三个月前就做这道题了, 但当时没得到flag, 在其他大佬做出来后, 赶紧来学习记录一波。

Ezsql

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。

靶机信息

剩余时间: 9663s

<http://1e926e68-fe73-4d08-827c-21262921d1b5.node4.buuoj.cn:81>

1e926e68-fe73-4d08-827c-21262921d1b5.node4.buuoj.cn:25883

<http://e445a3ea-f018-4222-a54c-dfb28dd032fa.node4.buuoj.cn:81>

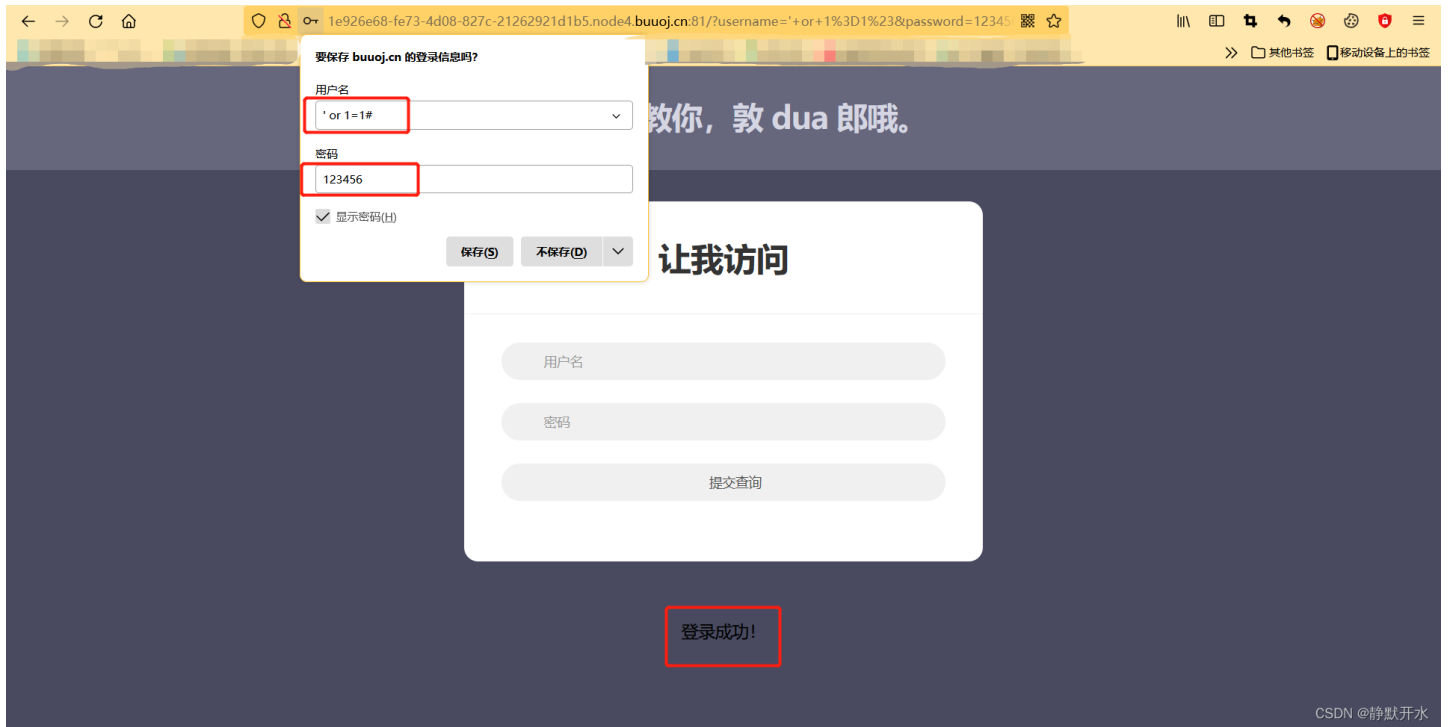
销毁靶机

靶机续期

已解锁

CSDN @静默开水

1. 题目的条件要求都写的很清楚了：web服务有漏洞，需要加固，加固成功可以访问一个地址得到flag
2. 首先访问web服务地址，发现是一个登录页面，立马尝试SQL注入，万能密码成功登录，明显存在注入漏洞。



3. 接下来SSH连接上目标机器地址, 查看目录, 找到登录页面代码进行代码审计, 找到用户登录的验证代码和SQL语句, 发现没有对输入的用户名和密码进行过滤就直接放到SQL查询语句。明显的漏洞, 接下来就是对其进行添加过滤函数, 完成加固。

```

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
$ ls /
bin  dev  flag.sh  lib  media  opt  root  sbin  start.sh  tmp  var
boot  etc  home  lib64  mnt  proc  run  srv  sys  usr
$ ls /var/www/html
css  dbConnect.php  fonts  index.php  js
$ cat /var/www/html/index.php
<!DOCTYPE html>
<html lang="zh">
<head>
  <meta charset="UTF-8">
  <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>让我访问</title>
  <link href="http://cdn.bootcss.com/bootstrap/3.3.7/css/bootstrap.min.css" rel="stylesheet">
  <link href="http://cdn.bootcss.com/font-awesome/4.6.3/css/font-awesome.min.css" rel="stylesheet">
  <link rel="stylesheet" type="text/css" href="css/htmlleaf-demo.css">
  <style type="text/css">
    .form-bg {
      padding: 2em 0;
    }

    .form-horizontal {
      background: #ffffff;
      padding-bottom: 40px;

```

CSDN @静默开水

```

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

```

CSDN @静默开水

4. 找寻过滤函数，逐一尝试后，在使用addslashes()函数时成功加固。

addslashes() 函数

在每个双引号 (") 前添加反斜杠:

```
<?php
$str = addslashes('Shanghai is the "biggest" city in China. ');
echo($str);
?>
```

addslashes() 函数返回在预定义字符之前添加反斜杠的字符串。

预定义字符是:

- 单引号 (')
- 双引号 (")
- 反斜杠 (\)
- NULL

5. 在xshell中修改代码, 如下:

6. 之前一直做不出来, 可能是因为我直接把addslashes()函数加在赋值函数式子上, 导致一直加固失败。

```
$username = $_GET['username'];
$password = $_GET['password'];
//变成以下
$username = addslashes($_GET['username']);
$password = addslashes($_GET['password']);
```

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

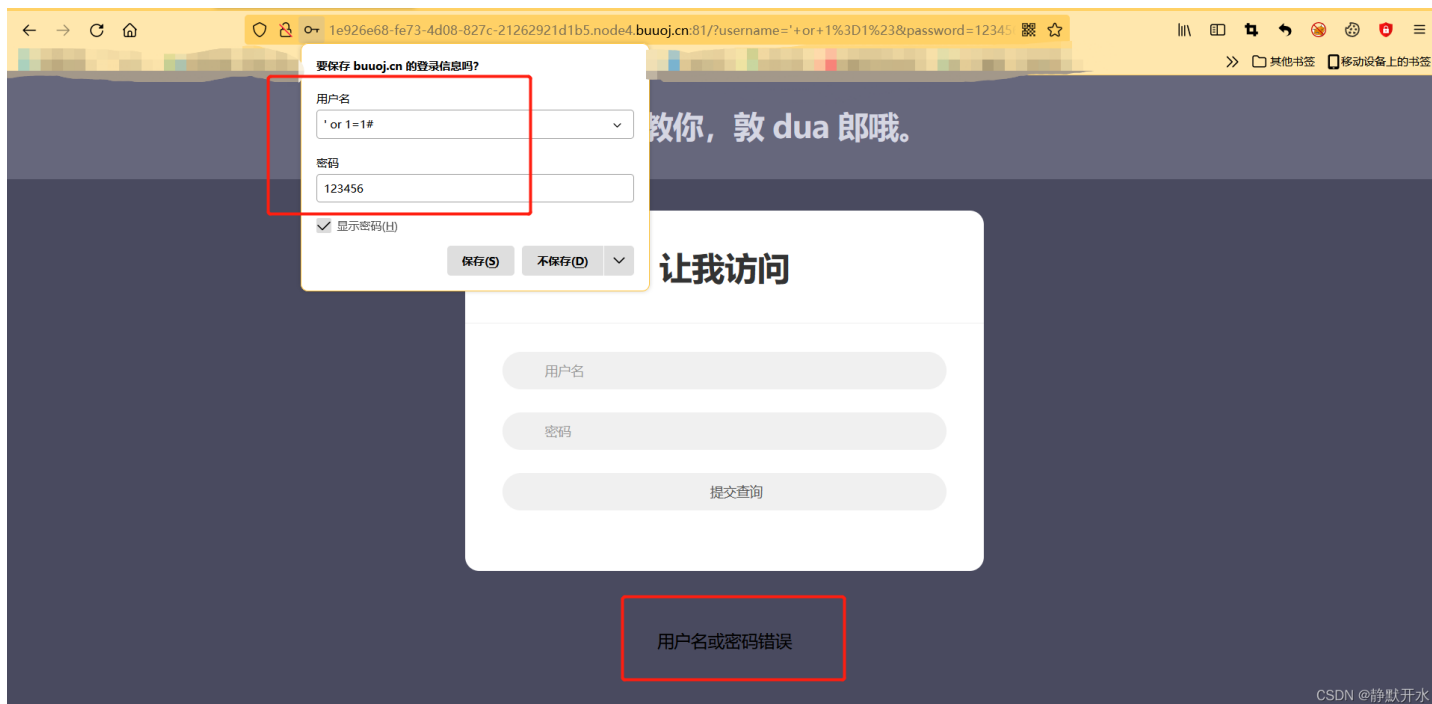


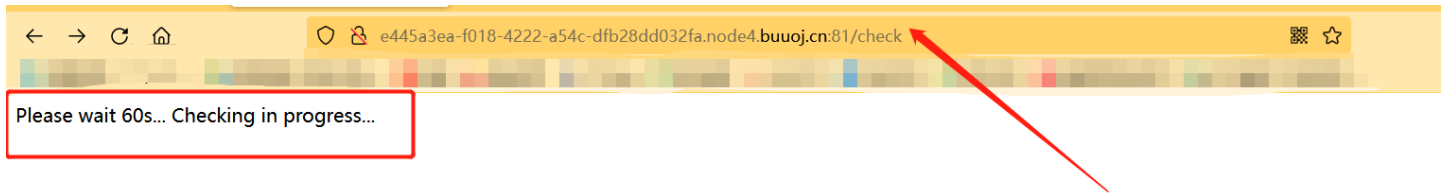
```
</div>
</div>
</body>
</html>
<h4 style="text-align: center; color: #000000">
<?php
error_reporting(0);
include 'dbConnect.php';
$username = $_GET['username'];
$password = $_GET['password'];

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

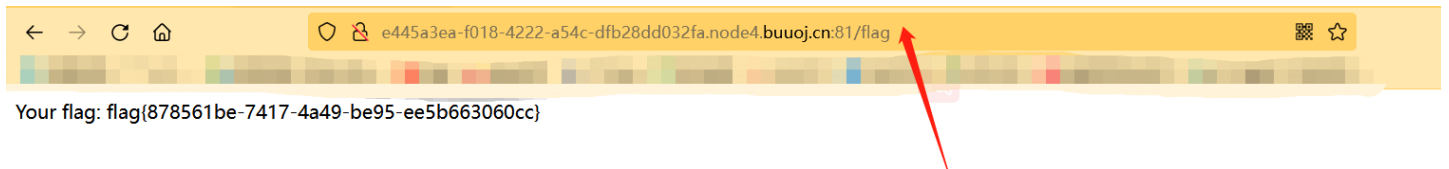
if (isset($_GET['username']) && isset($_GET['password'])) {
    $sql = "SELECT * FROM users WHERE username = '$username' AND password = '$password'";
    $result = $mysqli->query($sql);
    if (!$result)
        die(mysqli_error($mysqli));
    $data = $result->fetch_all(); // 亼N纒S舜~\榭~F中鱧·住~V璜~@舜~I录°璜®
    if (!empty($data)) {
        echo '馮»彈U彈~P倭~_[]A';
    } else {
        echo "潔”彈·佐~M彈~V宾F差~A麟~Y誤";
    }
}
?>
-- INSERT --
```

7. 加固后再次用万能钥匙进行登录，显示登陆失败，加固成功。





CSDN @静默开水



CSDN @静默开水

8. 访问Check 服务访问地址，得到flag。