BUUCTF 加固题 Ezsql WriteUp

原创

CVE-柠檬i 已于 2022-02-06 00:01:08 修改 3817 收藏 2

分类专栏： 安全 文章标签： web安全 安全 ctf sql注入 漏洞修复

于 2022-01-15 23:33:48 首次发布

本文链接：https://blog.csdn.net/weixin_49125123/article/details/122517483

文章目录

想直接要加固代码的点这里

题目

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

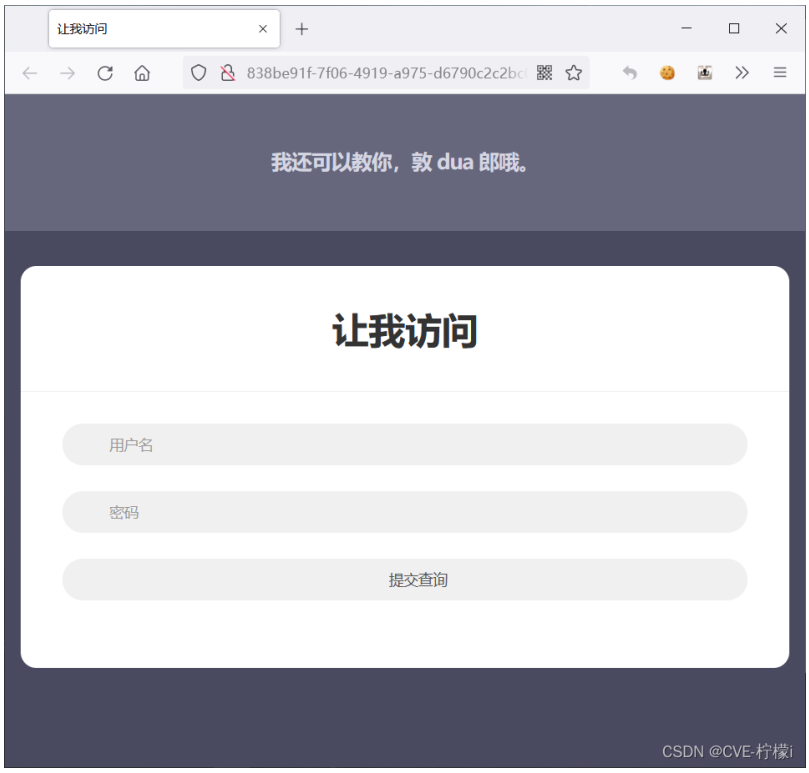
第三行：Check 服务访问地址

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、查看

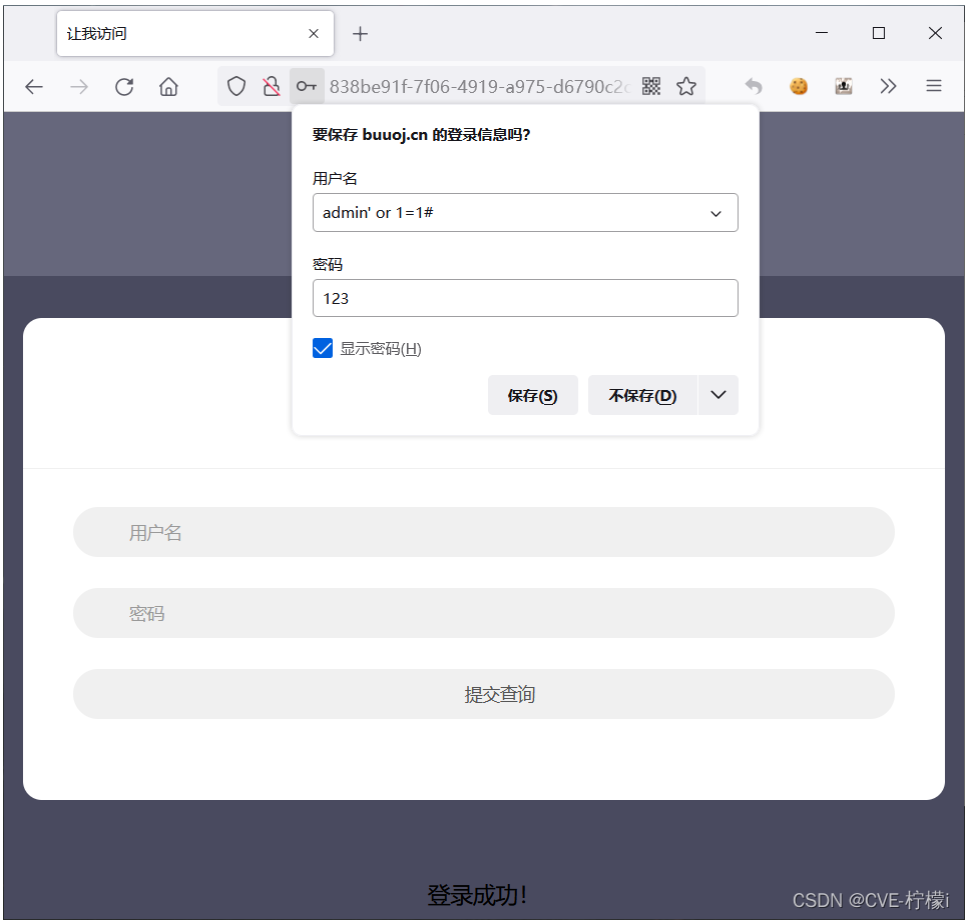
访问目标机器web服务地址，发现是一个登陆界面



利用万能密码登录成功

用户名：`admin' or 1=1#`

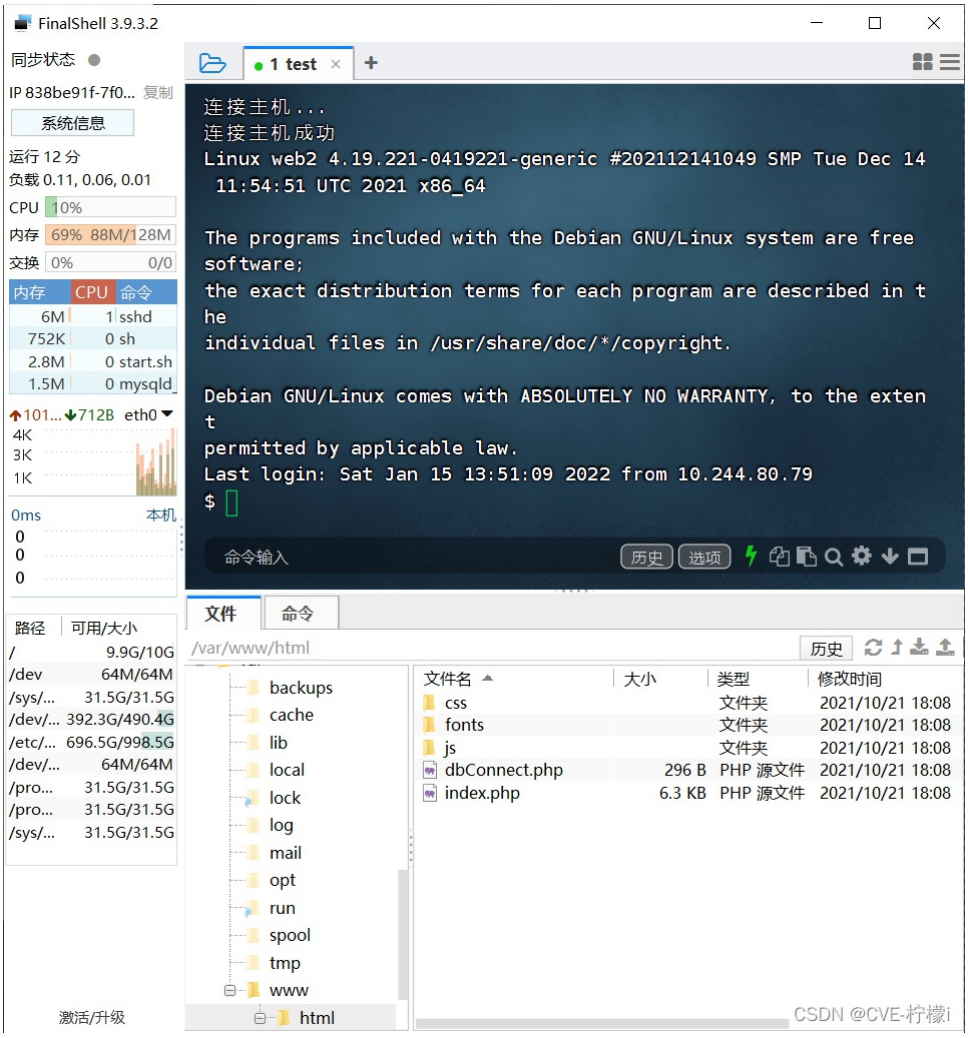
密码：`任意`



登陆成功，本题就是让加固这个登陆界面，以防止sql注入即可获取flag。

二、进入目标机器加固

根据给的地址和端口ssh连接目标机器，进入/var/www/html目录



加固index.php，查看它的源码

修改前的文件：

```
<!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/htmleaf-demo.css">
    <style type="text/css">
        .form-bg {
            padding: 2em 0;
        }

        .form-horizontal {
            background: #ffffff;
            padding-bottom: 40px;
            border-radius: 15px;
            text-align: center;
        }
```

```
.form-horizontal .heading {
    display: block;
    font-size: 35px;
    font-weight: 700;
    padding: 35px 0;
    border-bottom: 1px solid #f0f0f0;
    margin-bottom: 30px;
}

.form-horizontal .form-group {
    padding: 0 40px;
    margin: 0 0 25px 0;
    position: relative;
}

.form-horizontal .form-control {
    background: #f0f0f0;
    border: none;
    border-radius: 20px;
    box-shadow: none;
    padding: 0 20px 0 45px;
    height: 40px;
    transition: all 0.3s ease 0s;
}

.form-horizontal .form-control:focus {
    background: #e0e0e0;
    box-shadow: none;
    outline: 0 none;
}

.form-horizontal .form-group i {
    position: absolute;
    top: 12px;
    left: 60px;
    font-size: 17px;
    color: #c8c8c8;
    transition: all 0.5s ease 0s;
}

.form-horizontal .form-control:focus + i {
    color: #00b4ef;
}

.form-horizontal .fa-question-circle {
    display: inline-block;
    position: absolute;
    top: 12px;
    right: 60px;
    font-size: 20px;
    color: #808080;
    transition: all 0.5s ease 0s;
}

.form-horizontal .fa-question-circle:hover {
    color: #000;
}

.form-horizontal .main-checkbox {
```

```
.form-horizontal .main-checkbox {
    float: left;
    width: 20px;
    height: 20px;
    background: #11a3fc;
    border-radius: 50%;
    position: relative;
    margin: 5px 0 0 5px;
    border: 1px solid #11a3fc;
}

.form-horizontal .main-checkbox label {
    width: 20px;
    height: 20px;
    position: absolute;
    top: 0;
    left: 0;
    cursor: pointer;
}

.form-horizontal .main-checkbox label:after {
    content: "";
    width: 10px;
    height: 5px;
    position: absolute;
    top: 5px;
    left: 4px;
    border: 3px solid #fff;
    border-top: none;
    border-right: none;
    background: transparent;
    opacity: 0;
    -webkit-transform: rotate(-45deg);
    transform: rotate(-45deg);
}

.form-horizontal .main-checkbox input[type=checkbox] {
    visibility: hidden;
}

.form-horizontal .main-checkbox input[type=checkbox]:checked + label:after {
    opacity: 1;
}

.form-horizontal .text {
    float: left;
    margin-left: 7px;
    line-height: 20px;
    padding-top: 5px;
    text-transform: capitalize;
}

.form-horizontal .btn {
    float: right;
    font-size: 14px;
    color: #fff;
    background: #00b4ef;
    border-radius: 30px;
    padding: 10px 25px;
    border: none;
```

```
            text-transform: capitalize;
            transition: all 0.5s ease 0s;
        }

        @media only screen and (max-width: 479px) {
            .form-horizontal .form-group {
                padding: 0 25px;
            }

            .form-horizontal .form-group i {
                left: 45px;
            }

            .form-horizontal .btn {
                padding: 10px 20px;
            }
        }
    </style>
</head>
<body>
<div class="htmleaf-container">
    <header class="htmleaf-header">
        <h1>我还可以教你，敦 dua 郎哦。</h1>
        <div class="htmleaf-links">
        </div>
    </header>
    <div class="demo form-bg">
        <div class="container">
            <div class="row">
                <div class="col-md-offset-3 col-md-6">
                    <form class="form-horizontal" method="get" action="">
                        <span class="heading">让我访问</span>
                        <div class="form-group">
                            <input type="text" class="form-control" id="inputEmail3" placeholder="用户名" name="
username">
                        </div>
                        <div class="form-group help">
                            <input type="password" class="form-control" id="inputPassword3" placeholder="密码"
                                   name="password">
                        </div>
                        <div class="form-group help">
                            <input type="submit" class="form-control" id="inputSubmit">
                        </div>
                    </form>
                </div>
            </div>
        </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>
```

添加如下代码：

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

以下是W3school对 addslashes() 函数 的解释

> 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
>
> 该函数可用于为存储在数据库中的字符串以及数据库查询语句准备字符串。

修改后的文件

```
<!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/htmleaf-demo.css">
    <style type="text/css">
        .form-bg {
            padding: 2em 0;
        }

        .form-horizontal {
            background: #ffffff;
            padding-bottom: 40px;
            border-radius: 15px;
            text-align: center;
        }
```

```
.form-horizontal .heading {
    display: block;
    font-size: 35px;
    font-weight: 700;
    padding: 35px 0;
    border-bottom: 1px solid #f0f0f0;
    margin-bottom: 30px;
}

.form-horizontal .form-group {
    padding: 0 40px;
    margin: 0 0 25px 0;
    position: relative;
}

.form-horizontal .form-control {
    background: #f0f0f0;
    border: none;
    border-radius: 20px;
    box-shadow: none;
    padding: 0 20px 0 45px;
    height: 40px;
    transition: all 0.3s ease 0s;
}

.form-horizontal .form-control:focus {
    background: #e0e0e0;
    box-shadow: none;
    outline: 0 none;
}

.form-horizontal .form-group i {
    position: absolute;
    top: 12px;
    left: 60px;
    font-size: 17px;
    color: #c8c8c8;
    transition: all 0.5s ease 0s;
}

.form-horizontal .form-control:focus + i {
    color: #00b4ef;
}

.form-horizontal .fa-question-circle {
    display: inline-block;
    position: absolute;
    top: 12px;
    right: 60px;
    font-size: 20px;
    color: #808080;
    transition: all 0.5s ease 0s;
}

.form-horizontal .fa-question-circle:hover {
    color: #000;
}

.form-horizontal .main-checkbox {
    float: left;
```

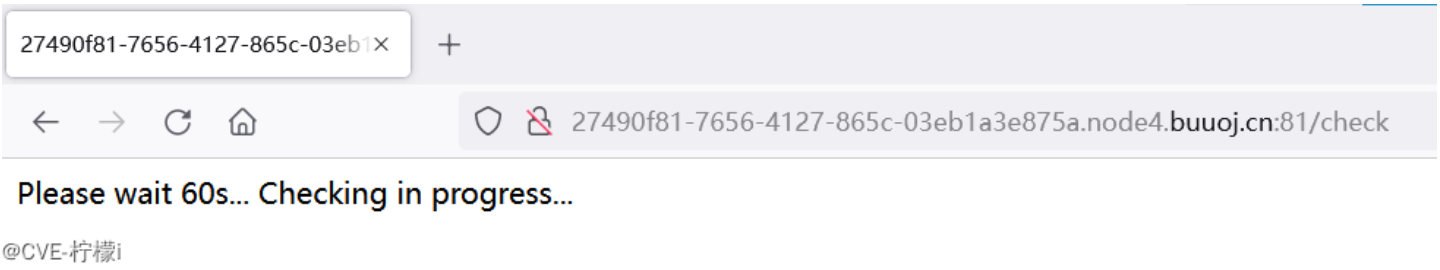
```
    float: left;
    width: 20px;
    height: 20px;
    background: #11a3fc;
    border-radius: 50%;
    position: relative;
    margin: 5px 0 0 5px;
    border: 1px solid #11a3fc;
}

.form-horizontal .main-checkbox label {
    width: 20px;
    height: 20px;
    position: absolute;
    top: 0;
    left: 0;
    cursor: pointer;
}

.form-horizontal .main-checkbox label:after {
    content: "";
    width: 10px;
    height: 5px;
    position: absolute;
    top: 5px;
    left: 4px;
    border: 3px solid #fff;
    border-top: none;
    border-right: none;
    background: transparent;
    opacity: 0;
    -webkit-transform: rotate(-45deg);
    transform: rotate(-45deg);
}

.form-horizontal .main-checkbox input[type=checkbox] {
    visibility: hidden;
}

.form-horizontal .main-checkbox input[type=checkbox]:checked + label:after {
    opacity: 1;
}

.form-horizontal .text {
    float: left;
    margin-left: 7px;
    line-height: 20px;
    padding-top: 5px;
    text-transform: capitalize;
}

.form-horizontal .btn {
    float: right;
    font-size: 14px;
    color: #fff;
    background: #00b4ef;
    border-radius: 30px;
    padding: 10px 25px;
    border: none;
    text-transform: capitalize;
```

```
            transition: all 0.5s ease 0s;
        }

        @media only screen and (max-width: 479px) {
            .form-horizontal .form-group {
                padding: 0 25px;
            }

            .form-horizontal .form-group i {
                left: 45px;
            }

            .form-horizontal .btn {
                padding: 10px 20px;
            }
        }
    </style>
</head>
<body>
<div class="htmleaf-container">
    <header class="htmleaf-header">
        <h1>我还可以教你，敦 dua 郎哦。</h1>
        <div class="htmleaf-links">
        </div>
    </header>
    <div class="demo form-bg">
        <div class="container">
            <div class="row">
                <div class="col-md-offset-3 col-md-6">
                    <form class="form-horizontal" method="get" action="">
                        <span class="heading">让我访问</span>
                        <div class="form-group">
                            <input type="text" class="form-control" id="inputEmail3" placeholder="用户名" name="
username">
                        </div>
                        <div class="form-group help">
                            <input type="password" class="form-control" id="inputPassword3" placeholder="密码"
                                   name="password">
                        </div>
                        <div class="form-group help">
                            <input type="submit" class="form-control" id="inputSubmit">
                        </div>
                    </form>
                </div>
            </div>
        </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'];

$
```

```
$username = addslashes($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、Check

再次进行万能密码登录发现已经不行了，然后就访问Check服务进行check



然后访问flag，发现flag已经出来了