

OWASP Juice Shop 一星难度 writeup

原创

[neversec](#) 于 2018-04-20 19:21:33 发布 1648 收藏

分类专栏: [CTF](#) 文章标签: [CTF](#) [OWASP](#) [信息安全](#)

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/github_35912913/article/details/80022990

版权



[CTF 专栏收录该内容](#)

4 篇文章 0 订阅

订阅专栏

近日在OWASP官网发现了这个靶场, 融入了OWASP TOP10的漏洞, 感觉好像很好玩, 花了好几天的时间自己快速地过了一遍。整理一哈wp发出来

环境搭建

官方的Github源码链接为 <https://github.com/bkimminich/juice-shop/>

源码NPM安装

注意 Node8 和 Node9 有所不同, 具体可见github的安装指南。以下是9的安装步骤

1. 安装 [node.js](#)
2. 下载源码 `git clone https://github.com/bkimminich/juice-shop.git`
3. `cd juice-shop`
4. `npm install`
5. 运行 `npm start`
6. 访问 <http://localhost:3000> 即可。

Docker安装 (推荐)

之所以推荐这个是因为挂掉了或者是重新开始也能很快地搭建环境。docker使用非常简单:

1. 安装 [Docker](#)
2. 拉取镜像 `docker pull bkimminich/juice-shop`
3. 运行容器 `docker run -d -p 3000:3000 bkimminich/juice-shop`
4. 访问 <http://localhost:3000> (遇到问题可以到Github上面看看安装指南)

一星难度

Score Board 计分板

Find the carefully hidden 'Score Board' page.找到仔细隐藏的“评分板”页面

对于新手来说, 根据这个页面可以让自己有目标地进行挖洞, 也是让自己有成就感的一种方式。:>

接下来gogogo:

在首页源代码发现了注释的一块代码：

```
<li class="dropdown ng-hide" ng-show="scoreBoardMenuVisible">
  <a href="/#/score-board">
    <svg class="svg-inline--fa fa-trophy fa-w-18 fa-lg"
      aria-hidden="true" data-prefix="fas" data-icon="trophy" role="img" xmlns="http://www.w3.org/2000/svg" viewBox="0 0 576 512" data-fa-i2svg="">
    </svg>
    <!--<i class="fas fa-trophy fa-lg"></i-->
    <span class="ng-scope" translate="TITLE_SCORE_BOARD">
      计分板</span>
    </a>
  </li>
```

访问该页面 </#/score-board> 会跳到计分板，里面有各个难度的说明

OWASP Juice Shop v7.0.2

登录 中文 搜索... 搜索 联系我们 计分板 关于我们

你成功地解决了一项挑战：Score Board (Find the carefully hidden 'Score Board' page.)

计分板

2%

难度系数

1^{1/7} 2^{0/8} 3^{0/13} 4^{0/15} 5^{0/10} 6^{0/6}

名称	描述	状态
Admin Section	Access the administration section of the store.	未解决
Confidential Document	Access a confidential document.	未解决
Error Handling	Provoke an error that is not very gracefully handled.	未解决
Redirects Tier 1	Let us redirect you to a donation site that we...	未解决
Score Board	Find the carefully hidden 'Score Board' page.	未解决
XSS Tier 1	Perform a <i>reflected</i> XSS attack with <code><script></code>	未解决
Zero Stars	Give a devastating zero-star feedback to the s...	未解决

This website uses fruit cookies to ensure you have the juiciest tracking experience. [But me want it!](#)

Admin Section 管理员页面

Access the administration section of the store. 访问商店的管理页面。

找到后台管理页面。御剑走一波扫不出来，根据描述猜解访问了 <http://192.168.209.146:3000/administration>，结果发现不行，重新输入 <http://192.168.209.146:3000/#/administration> 访问成功



结果完成了两个（挠头）

Confidential Document 机密文件

Access a confidential document. 访问机密文件

看到这个一开始不知道哪儿有，搁置了一边之后在中途看到了这个链接：

关于我们 公司的历史和政策

Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui blandit praesent luptatum zzril delenit augue duis dolore te feugait nulla facilisi. 如果你在厕所闷得慌, 就看看我们无聊的使用条款。 Nam liber tempor cum soluta nobis eleifend option congue nihil imperdiet doming id quod mazim placerat facer possim assum. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet

可能是因为中文的原因, 这一行真的太明显了吧。。点开链接 http://192.168.209.146:3000/ftp/legal.md?md_debug=true

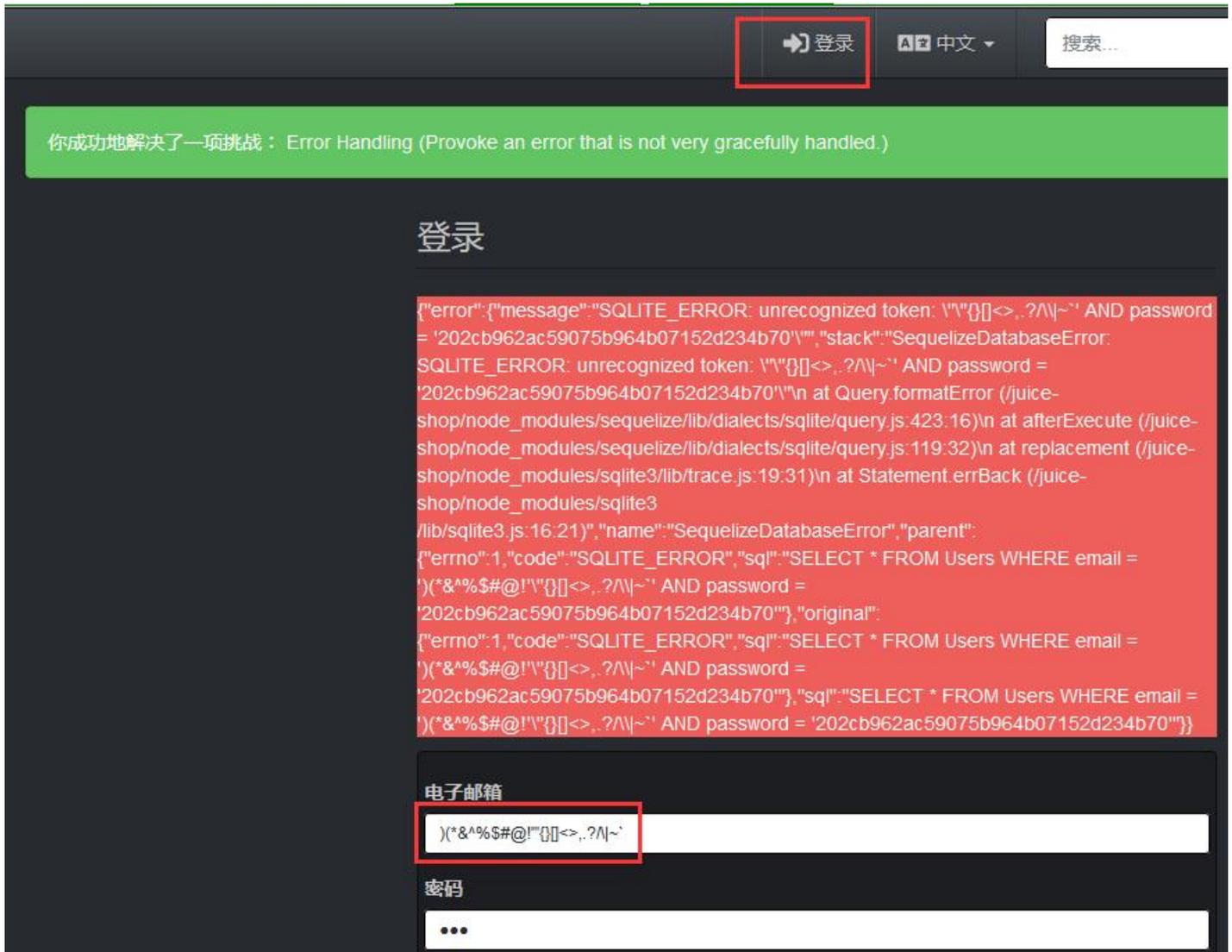
访问<http://192.168.209.146:3000/ftp> 发现可以直接访问其ftp目录

点开一些文件提示 `403 Error: Only .md and .pdf files are allowed!`, 这个点是访问了第一个md文件就可以过了。此处还发现了一些bak文件, 这个漏洞下面会说到

Error Handling 错误处理

Provoke an error that is not very gracefully handled. 提出一个不太适合处理的错误。

题目的意思是寻找出报错页面，由于上面莫名其妙完成了有点不知所以，docker重置了一波环境，在登录处看到了报错：



报错后即可完成

Redirects Tier 1 重定向第一关

Let us redirect you to a donation site that went out of business. 让我们将您重定向至停业的捐赠网站。

后续测试过程在购物车页面找到注释的重定向网址，实在是太猥琐了

```
<!--<a href="/redirect?to=https://gratipay.com/juice-shop" target="_blank" class="btn btn-danger">
  <i class="fab fa-gratipay fa-lg"></i> Gratipay
</a-->
```

XSS Tier 1 XSS第一关

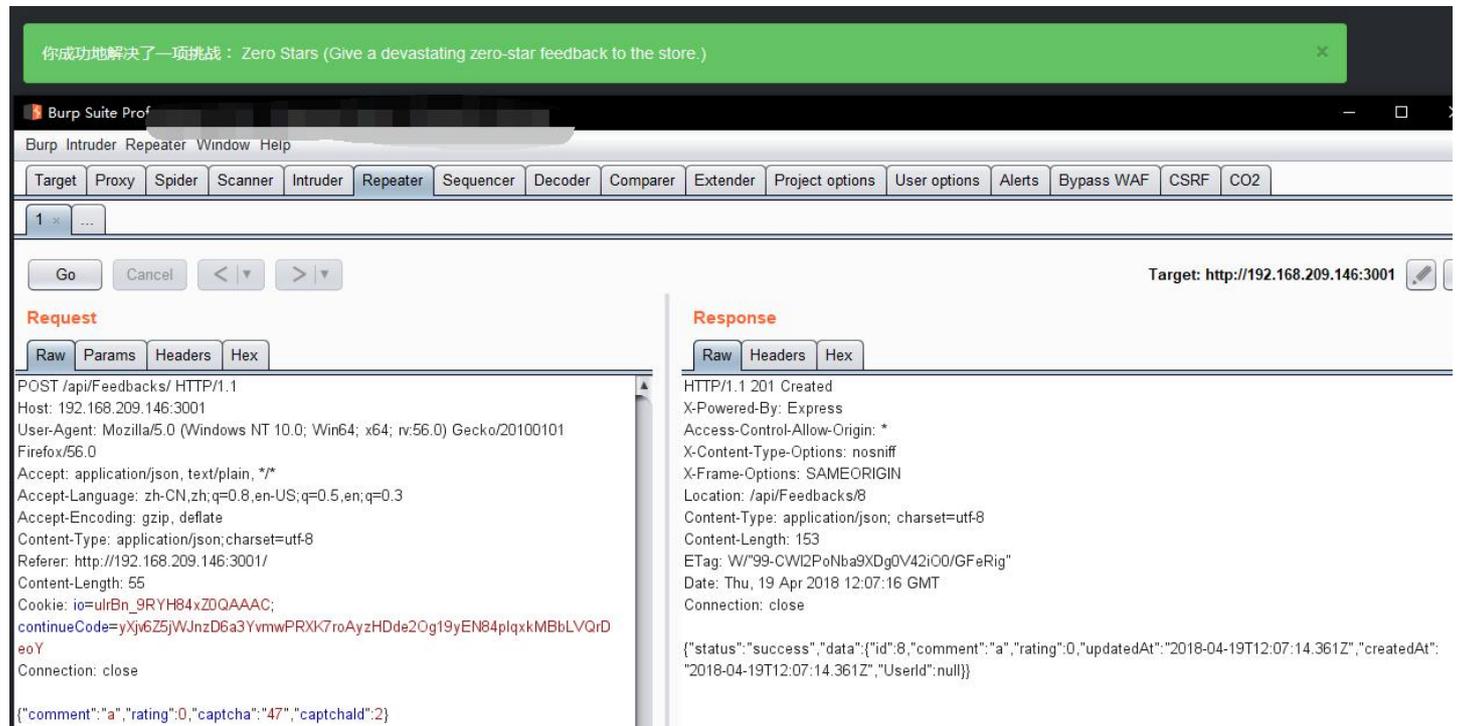
Perform a reflected XSS attack with . 执行反射 XSS攻击 <script>alert("XSS")</script> 。

搜索框直接可以弹，闭合了反而没有提示完成，略坑=。=

Zero Stars 零星评价

Give a devastating zero-star feedback to the store. 给商店带来毁灭性的零星反馈。

评价链接位于 联系我们 <http://192.168.209.146:3001/#/contact>, burp改包可过



你成功地解决了一项挑战：Zero Stars (Give a devastating zero-star feedback to the store.)

Burp Suite Prof

Target: <http://192.168.209.146:3001>

Request

Raw Params Headers Hex

```
POST /api/Feedbacks/ HTTP/1.1
Host: 192.168.209.146:3001
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: application/json, text/plain, /*
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf-8
Referer: http://192.168.209.146:3001/
Content-Length: 55
Cookie: io=ulrBn_9RYH84xZ0QAAAC;
continueCode=yXjv6Z5jWJnzD6a3YvmwPRXk7roAyzHDde2Og19yEN84plqXkMBbLVQrDeoY
Connection: close

{"comment":"a","rating":0,"captcha":"47","captchald":2}
```

Response

Raw Headers Hex

```
HTTP/1.1 201 Created
X-Powered-By: Express
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Location: /api/Feedbacks/8
Content-Type: application/json; charset=utf-8
Content-Length: 153
ETag: W/"99-CWl2PoNba9XDg0V42i00/GFeRig"
Date: Thu, 19 Apr 2018 12:07:16 GMT
Connection: close

{"status":"success","data":{"id":8,"comment":"a","rating":0,"updatedAt":"2018-04-19T12:07:14.361Z","createdAt":"2018-04-19T12:07:14.361Z","UserId":null}}
```