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

本文链接：https://blog.csdn.net/github_35912913/article/details/80022990

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

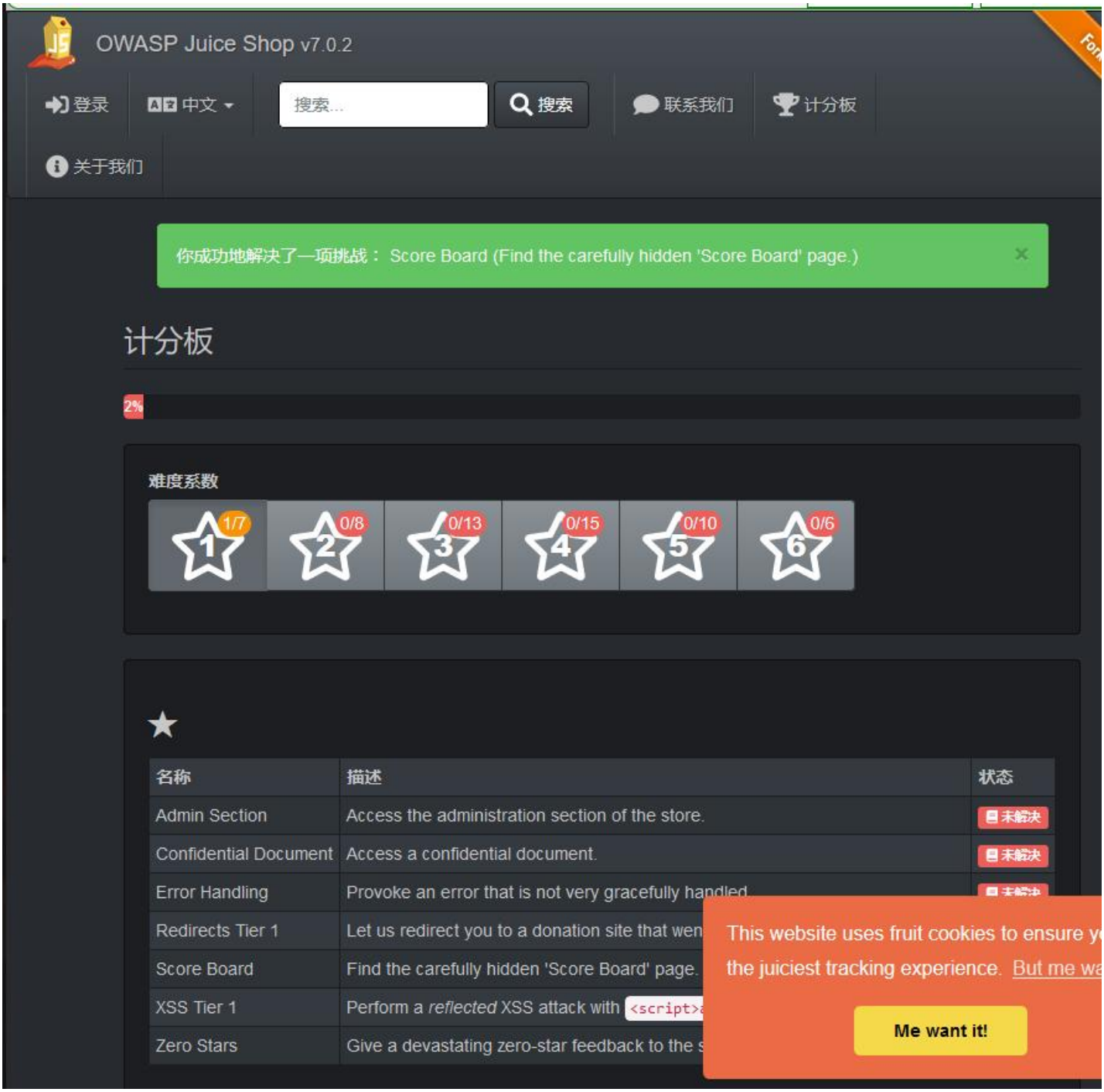
> Find the carefully hidden ‘Score Board’ page.找到仔细隐藏的“评分板”页面

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：

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



Admin Section 管理员页面

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

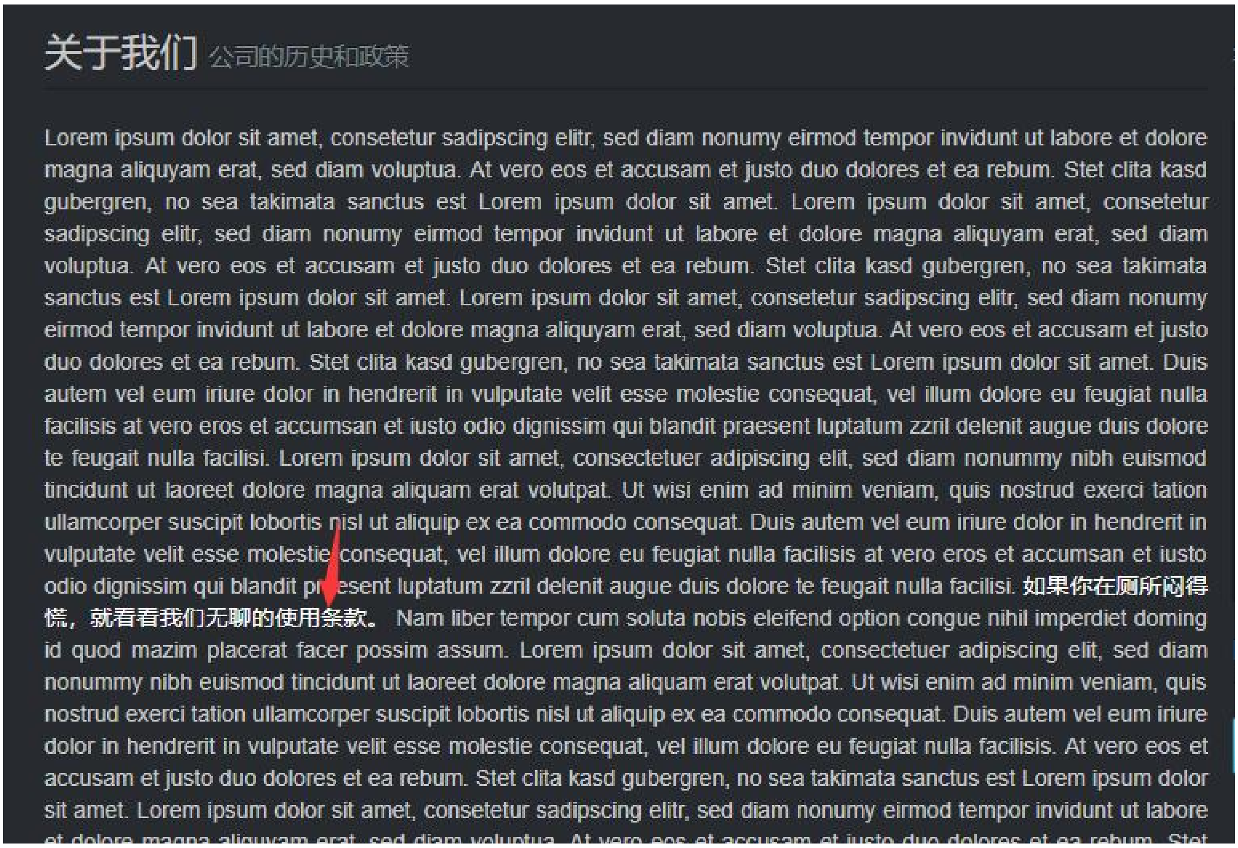
找到后台管理页面。御剑走一波扫不出来，根据描述猜解访问了 http://192.168.209.146:3000/administration，结果发现不行，重新输入 http://192.168.209.146:3000/#/administration 访问成功

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：



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

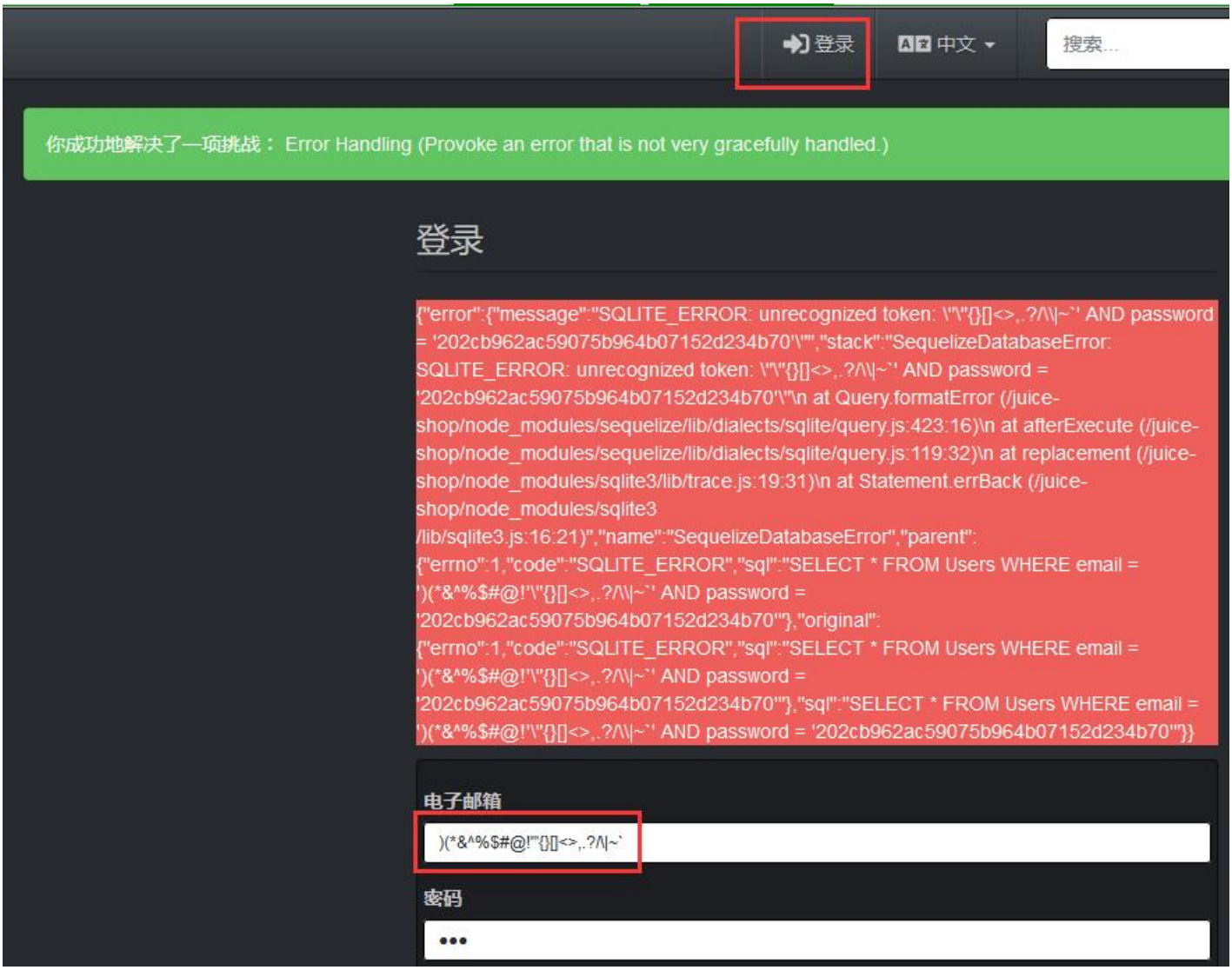
访问http://192.168.209.146:3000/ftp 发现可以直接访问其ftp目录

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