OWASP Juice Shop 二星难度 writeup

原创

neversec 于 2018-12-12 11:39:16 发布 957 收藏

分类专栏： CTF 信息安全 文章标签： CTF Juice shop OWASP 信息安全 靶场

本文链接：https://blog.csdn.net/github_35912913/article/details/84969937

前言

本writeup所有题目基于**OWASP Juice shop V7.0.2**，靶场更新较快，后续有新的题目会接着更新。

点此看一星难度wp

二星难度

Basket Access 购物车访问

> Access someone else's basket. 访问他人的购物车

修改会话存储的bid，访问购物车即可

Christmas Special 圣诞特别礼

> Order the Christmas special offer of 2014. 订购2014年的圣诞特供

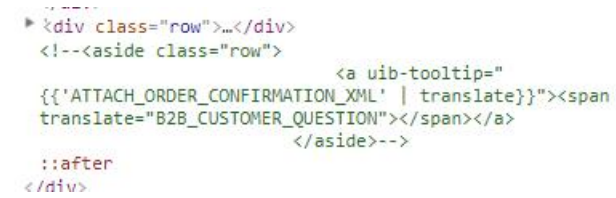
搜索框SQL注入。抓包回显了报错语句，明显有SQL注入

分析语句，构造payload为`q='))--`可以查询出所有商品，添加2014的圣诞特供商品即可

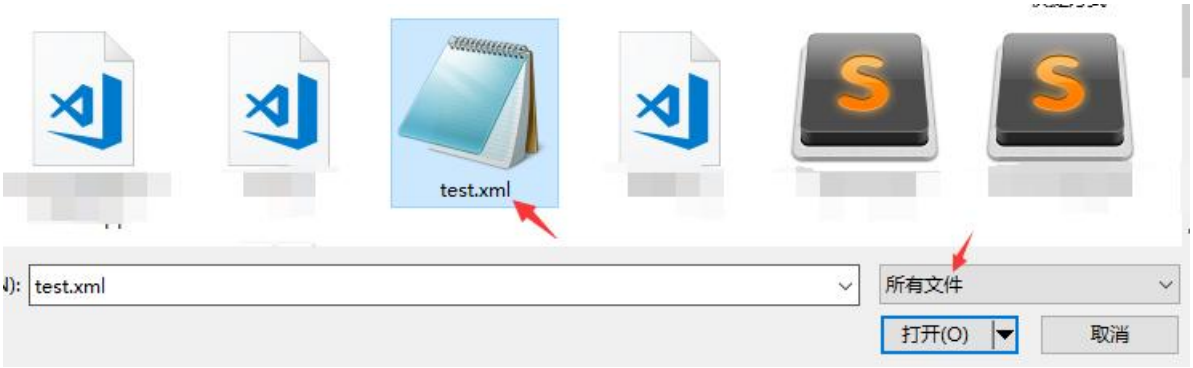
Deprecated Interface 已弃用的接口

> Use a deprecated B2B interface that was not properly shut down. 使用未正确关闭的废弃的B2B接口。

B2B接口不清楚是什么，但是在http://192.168.209.146:3001/#/complain页面中有一段注释掉的代码写着B2B，这个地方也可以上传xml文件，但是限定了只能从电脑选择pdf文件。



然而还是可以选xml文件进行上传



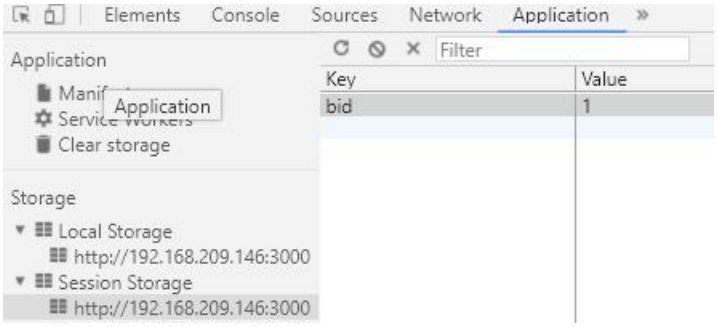
上传后返回了`410`状态码，但是挑战也成功了。

> 410：被请求的资源在服务器上已经不再可用，而且没有任何已知的转发地址。410响应的目的主要是帮助网站管理员维护网站，通知用户该资源已经不再可用，并且服务器拥有者希望所有指向这个资源的远端连接也被删除。

Five-Star Feedback 五星级的反馈

> Get rid of all 5-star customer feedback. 删掉所有的5星客户评价

在http://192.168.209.146:3000/#/administration页面上，修改bid为1，即可删除



Login Admin 登陆Admin

> Log in with the administrator's user account. 使用管理员用户账号登陆

只能是sql注入了。回到登陆框，抓包看到提交的数据为`{"email":"\" or 1=1--","password":"123"}`，结合sql语句`SELECT * FROM Users WHERE email = '1'' AND password = '202cb962ac59075b964b07152d234b70'`，payload为`email":"' or 1=1 --","password":"123"`即可使用管理员登陆。原因是管理员的数据在select结果处于第一位。

Login MC SafeSearch 登陆MC SafeSearch

> Log in with MC SafeSearch's original user credentials without applying SQL Injection or any other bypass. 使用MC SafeSearch的原始用户凭据登录，无需应用SQL注入或任何其他旁路。

一开始以为是注入，但是题目写了不用注入，最后我也没想到是社工，搜索了一波才知道。

首先有sql注入的话用户都可以枚举，我手动测试了一下，发现`{"email":"' or 1=1 limit 7,1 --","password":"123"}`就是MC SafeSearch的邮箱`mc.safesearch@juice-sh.op`，使用该payload。

谷歌搜索 MC SafeSearch，发现一个Rapper唱的关于密码强度的MV

播放视频开始切克闹，发现关键信息

于 视频 0:25 表示了使用宠物的名字`Mr.Noodles`作为密码，然后将一些字母变成了0，一般习惯是将 o 变成 0，所以密码就是`Mr. N00dles`。坑点之处在密码中间要加空格，令人头大。

Password Strength 密码强度

> Log in with the administrator's user credentials without previously changing them or applying SQL Injection. 使用管理员的用户凭证登录，而不必事先更改或应用SQL注入。

题目是密码强度，考察点是弱密码。购物篮中有管理员邮箱`admin@juice-sh.op`，使用burp爆破即可，注意爆破速度不要过快，很容易扫挂掉

Request	Payload	Status	Error	Timeout	Length
3425	admin123	200	☐	☐	891
0		401	☐	☐	330

Weird Crypto 奇怪的加密

> Inform the shop about an algorithm or library it should definitely not use the way it does. 告知商店一个算法或库，它绝对不应该使用它的方式。

在 http://192.168.209.146:3000/#/contact 提交一个不安全的算法。
这个答案一共有5个：z85 base85 base64 md5 hashid ，提交一个即可。

- md5: 数据库里面的密码是md5
- base64: google accounts注册时密码用的b64传输
- z85/hashid/base85: 六星难度题目出现的算法和库，后边会讲到