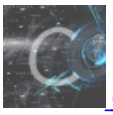
CTF总结

原创

小冻子 于 2021-10-14 22:26:45 发布 2129 收藏

分类专栏： CTF 文章标签： 安全漏洞

本文链接：https://blog.csdn.net/weixin_38418878/article/details/120773710



昨天参加了一场公司举办的CTF，虽是初级场，但是自己真正第一次参加，觉得甚是有意思，可惜没有参考答案，只能趁热记录下来自己挖出来的漏洞。

1. SQL注入

在输入框或者url里可以尝试SQL注入

譬如username中输入[\' or 1=1#] 便可免密登录，因为查询语句是 select * from DB where username='' or 1=1 # password='

#后面的内容被注释掉了，有时候–也可以用于注释。

2.xss攻击

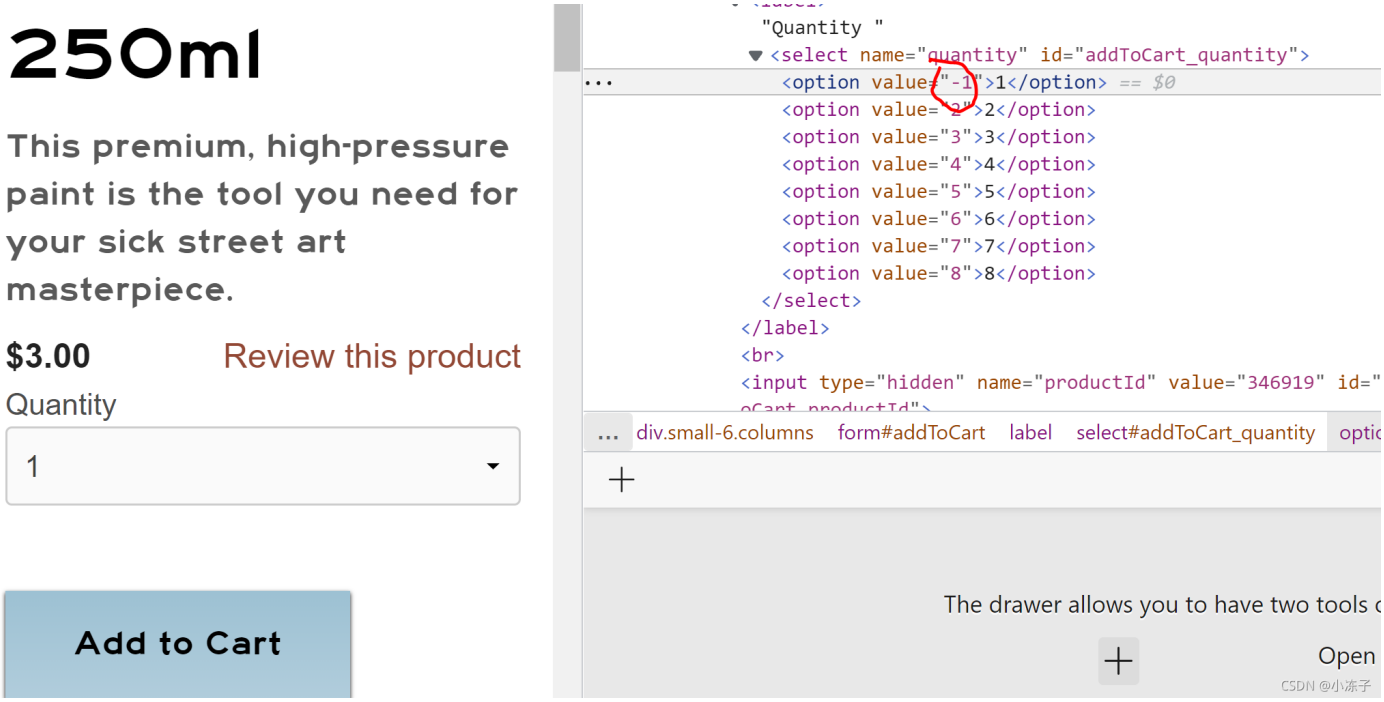
在输入框中尝试输入`<script>alert("XSS on Product Search");</script>`会执行个语句。

3.robots.txt

web根目录下输入robots.txt，尝试输入上面列出的Allow和Disallow的url

4. HTML

1）查看html的源代码，小心里面的`hidden`字样，它会帮你找到隐藏款。
譬如，`<input type="hidden" name="redirect" value="" id="doLogin_redirect">`
如果去掉了`type="hidden"`，在显示出的输入框中输入其他的网址，如`http://evil.com`，那么用户在登录的时候会自动跳转到其他的网站中。
2）更改html源代码，将购买的数量改成负数。还有价格，也可以更改成负数



3）也是更改html源代码，譬如登录别人的账户查看html代码得到了别人的信用卡对应的value，然后切换子的账户，将value改成别人的信用卡，用于付钱，

5. 更改URL

url除了可以注入之外，还要小心上面的id属性，尝试把id+1，-1，也许能看到别的账户的信息。
在看到别的账户的信息之后，可以尝试做一些删除等操作。

6.熟悉编码格式

譬如以==结尾，就要想到base64编码，还有常用的md5等，有的hash值直接在google搜，就能搜到解码后的数据，常用于破解密码。

7.上传不安全的文件

如果有上传文件的地方，可以上传一些不支持的格式。

8.CTF

这一part是我觉得最有意思的一part，因为它考验脑洞、观察力、推理能力等等，譬如我解出来的一个，点开所有的graph，发现有一个graph旁边写着一串摩斯密码，然后将那串密码反编译，得到了一串英文字符串，根据字符串的意思进行操作，最后得分了

由于作者水平有限，只挖出了这些漏洞，纯手工挖的，没使用其他的工具譬如ZAP BurpSuite等，用这些应该能挖出更多的漏洞，这一次挖出了一大半的漏洞，已经超出自己的预期了，期待以后继续参加吧！加油！