接口漏洞实战

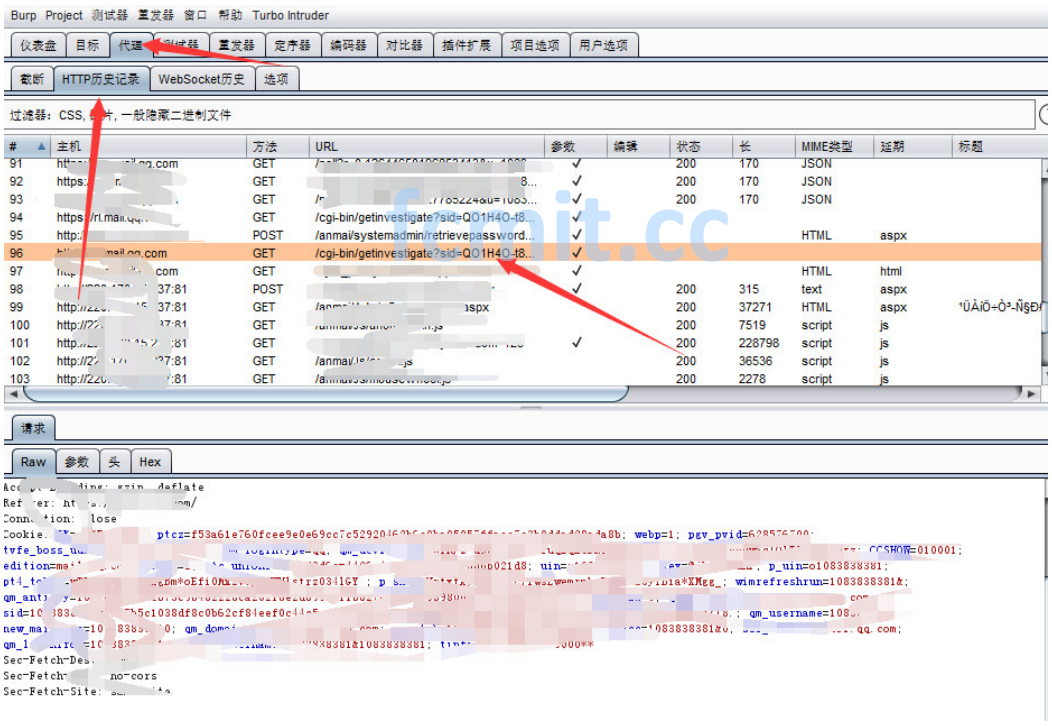
前言： 在我们信息收集获取 webvpn 或者 sslvpn 后，我们就可以进入一站式服务大厅进行漏洞挖掘。

一、漏洞介绍：

1.水平越权访问是一种“基于数据的访问控制”设计缺陷引起的漏洞。由于服务器端在接收到请求数据进行操作时没有判断数据的所属人/所属部门而导致的越权数据访问漏洞，**而这种越权最容易出现的位置就是？Id=（传参值） 和 post 传参的参数中，或者存在个人信息页面，个人资料这些隐藏的接口中**

2. 方法一：

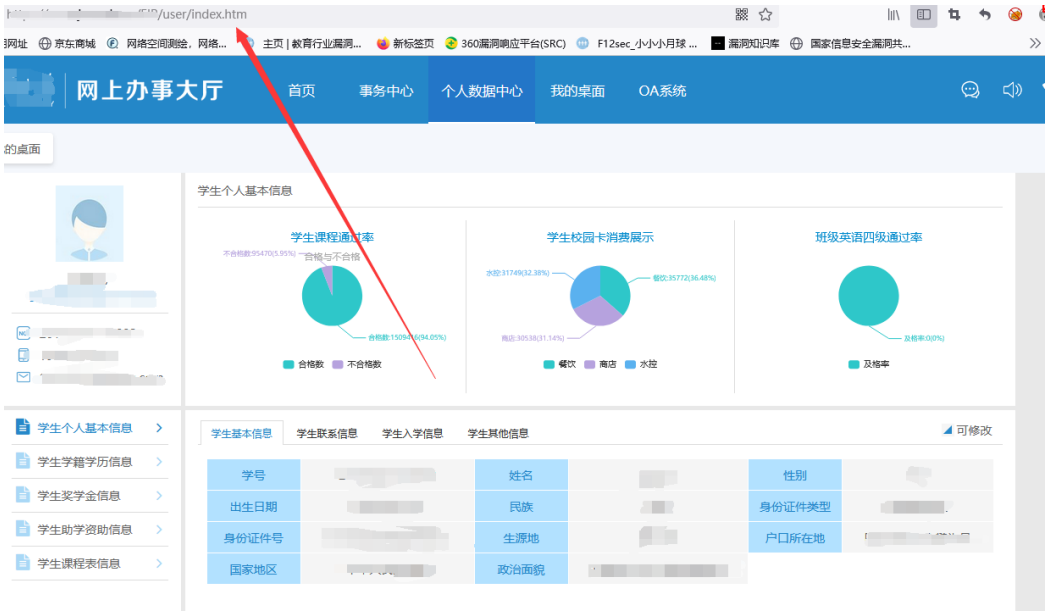
往往在挖掘过程程中，拿到同一个站点，别人能挖掘出水平越权或者垂直越权，而你却不能发现，那些因为这些越权漏洞的传参值都是接口在进行，所以我们在挖掘的过程中可以打开 burp 抓住每一个包，然后再去看 burp 中的 http 历史记录，查看接口信息，在进行测试



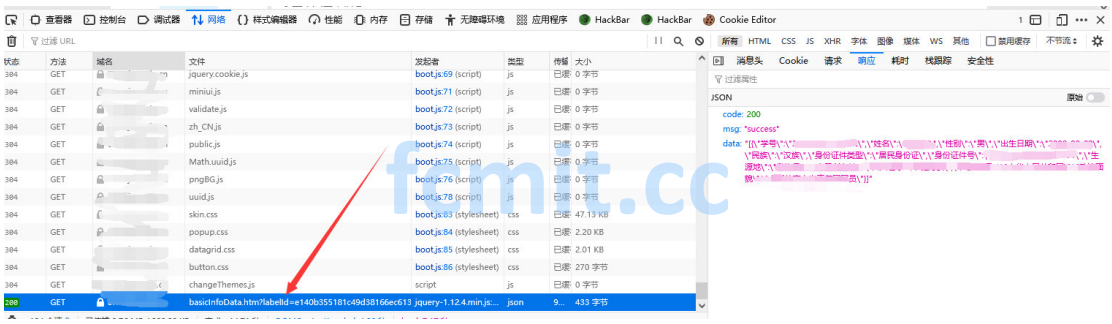
如上图一样，如果在站点页面是无法看见?sid 这个参数的，而你在 burp 历史包中即可以看见此参数，这个参数就是个人身份的参数，如果没鉴权，那么水平越权就到手。

方法二：

直接使用浏览器的控制台中的网络即可查找，比如：



可以看出这个页面，你根本没有任何办法测试水平越权，但是你可以通过查看接口的办法将个人信息的接口查找出来后进行测试：



调用后，你可以将参数？ablid=参数值换为别人的参数，即可测试存在越权不：

二、案例（某证书大学的挖掘）：

访问 webvpn:

https://[redacted]/https/77726476706e69737468656265737421f3f652d224236457300d8db9d6562d/cas/login

账号：[redacted]

漏洞站点：

https://[redacted]p/77726476706e69737468656265737421a1a70fce7f7e39002c46d8f8c0/Managers/DepartItemList.aspx?values=E211F2DDDD0D736FC2675D35A96CECED&rylb=1&flag=js

水平越权查看全校老师的个人信息：将 values 的值替换为别的即可

通过该站点：

https://[redacted]/http/77726476706e69737468656265737421a1a70fce7f7e39002c46d8f8c0/Telephonenumber.aspx?verify=6BE241A7B56631143719F26BAC55382A&userName=201700065&strSysDatetime=2021-08-0914:36:06&jsName=teacher&url=

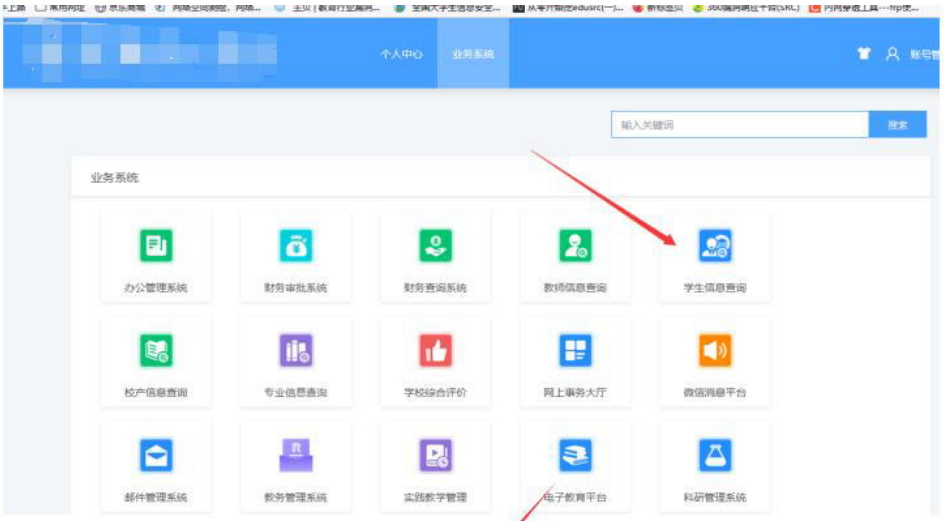
中的接口：

https://[redacted]p/77726476706e69737468656265737421a1a70fce7f7e39002c46d8f8c0/Handler/JSJCXX/QueryAllJSLists.ashx?vpn-12-o1-10.28.102.148

可以查看全校老师的 values:

（这次是打的组合拳，我都没有想到在 B 站点的接口中泄露全校师生的 values，所以在挖一个学校的时候，不要着急提交漏洞，应该慢慢的全部系统的都分析一下，遇见有用的就记录下来）

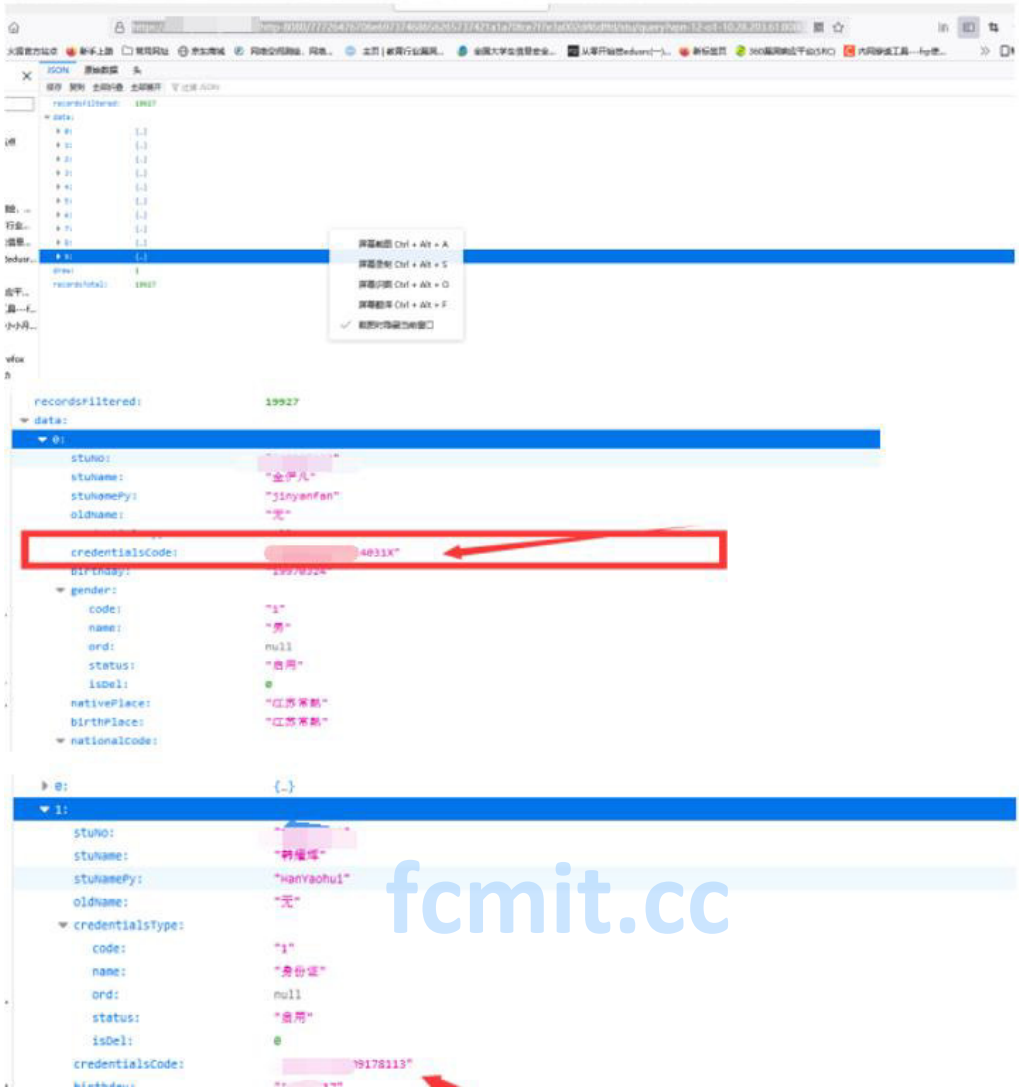
第二处漏洞：



进入后访问学生查询：

可以清楚的看见，sfz 是进行了加密处理的，但是你在 f12 查看个人接口的时候，你会发现接口中的数据全是清晰可见

可以查看全校学生个人信息包括身份证，和老师工号以及密码的 md5 值

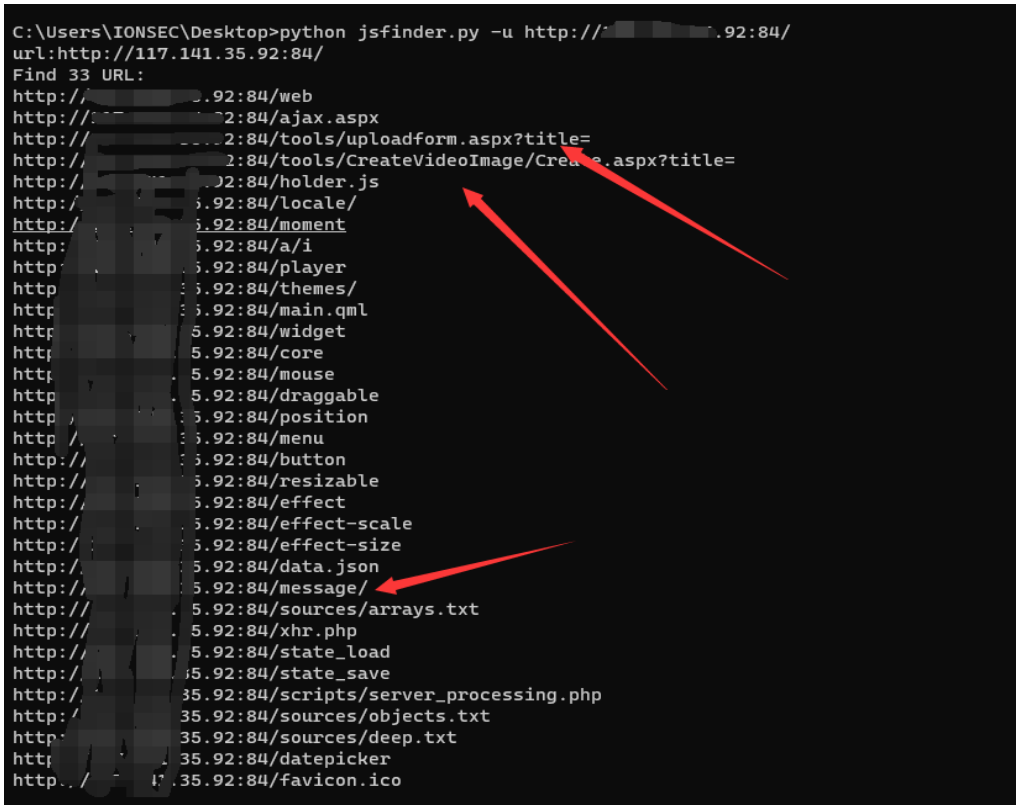


所以挖越权漏洞要多调用 burp 的历史记录或者 f12 查看接口，往往对接口的鉴权是程序员经常忽略的。

三、方法三使用脚本 jsfind 进行查找：

站点：

使用脚本：



可以看出很多接口，访问即可，有前台未授权上传和前台 ssrf 就不上图了