

记一次从0到1的edu通杀0day挖掘

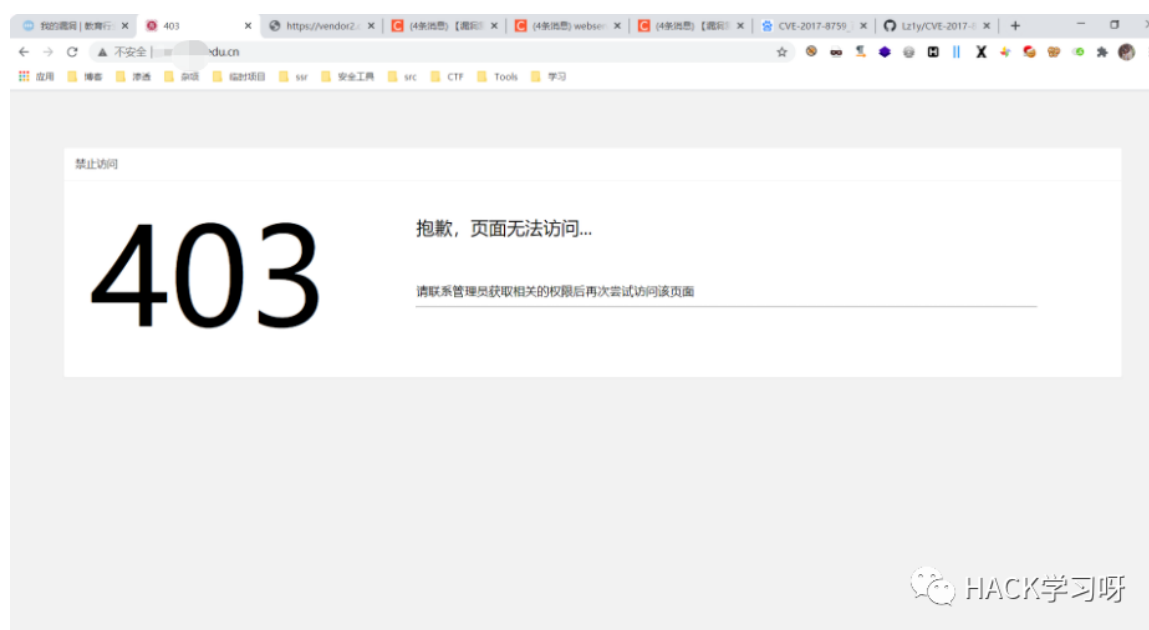
原创 Ma4ter HACK学习呀

2021-01-10原文

2021第一天就挖掘出来了0day 毕竟也是人生第一个0day 也是很开心

废话不多说 直接进入主题 全部漏洞网站已经提交edu src修复 思路仅供参考

我是从自己学校网站挖到的 只不过现在网站已经关了 于是就去找了个比较相似点的



当然挖掘漏洞肯定是一个漫长的过程 运气也很重要 得仔细

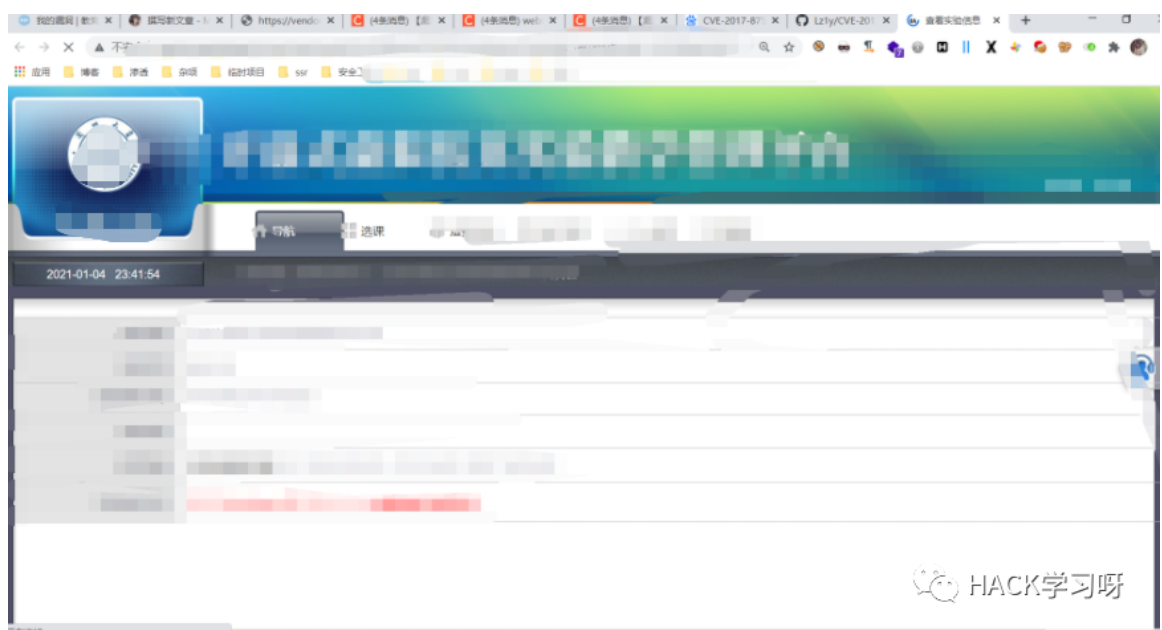
有什么功能点就去测什么点 数据包放bp上面多重放几道（个人见解 dalao勿喷）

当时差不多就找到一个这个点

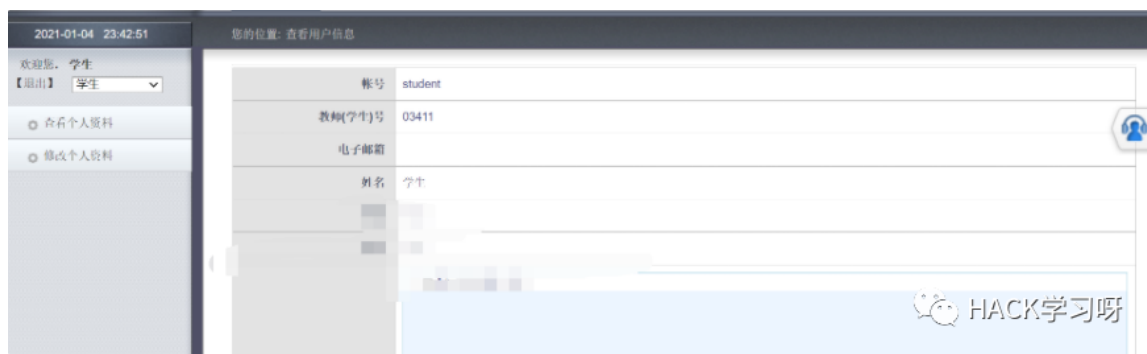




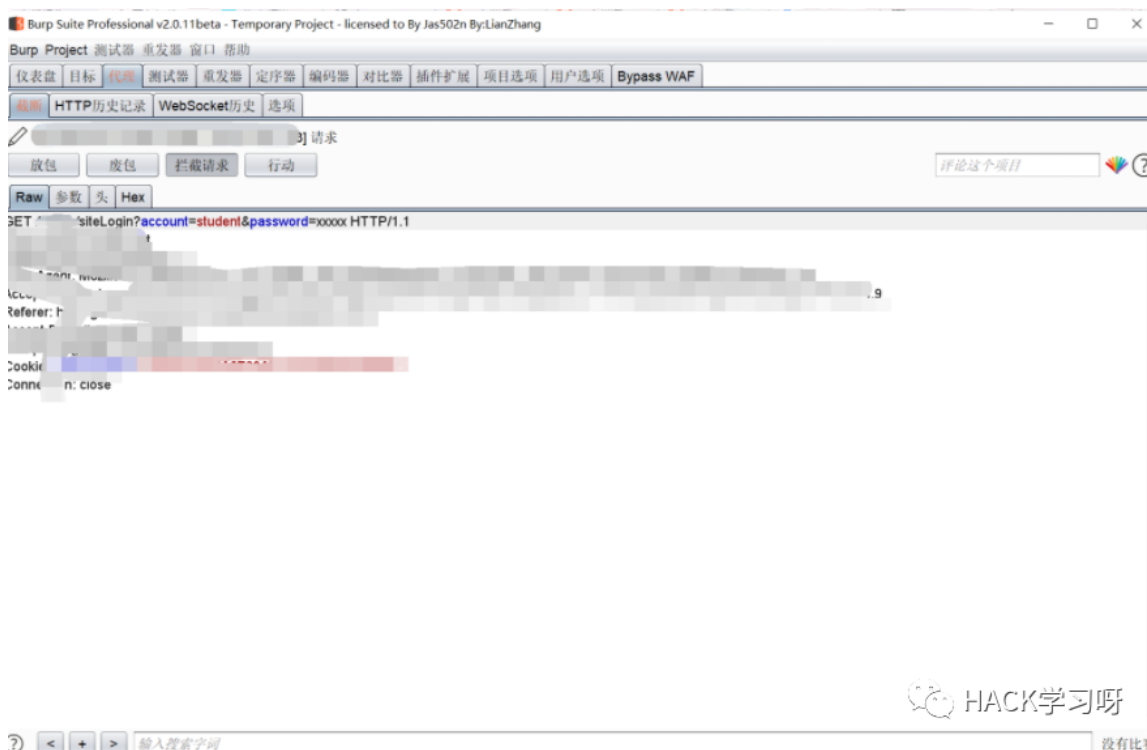
点进去发现直接进入后台了



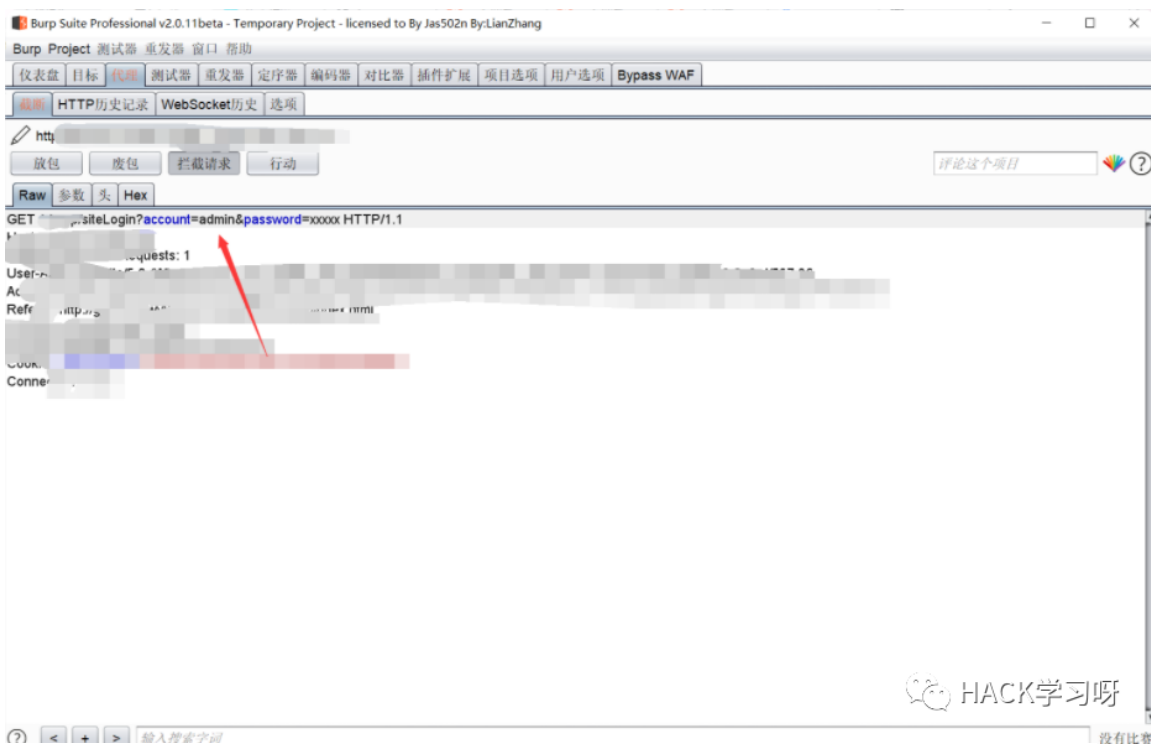
但是是一个权限很小的测试账户



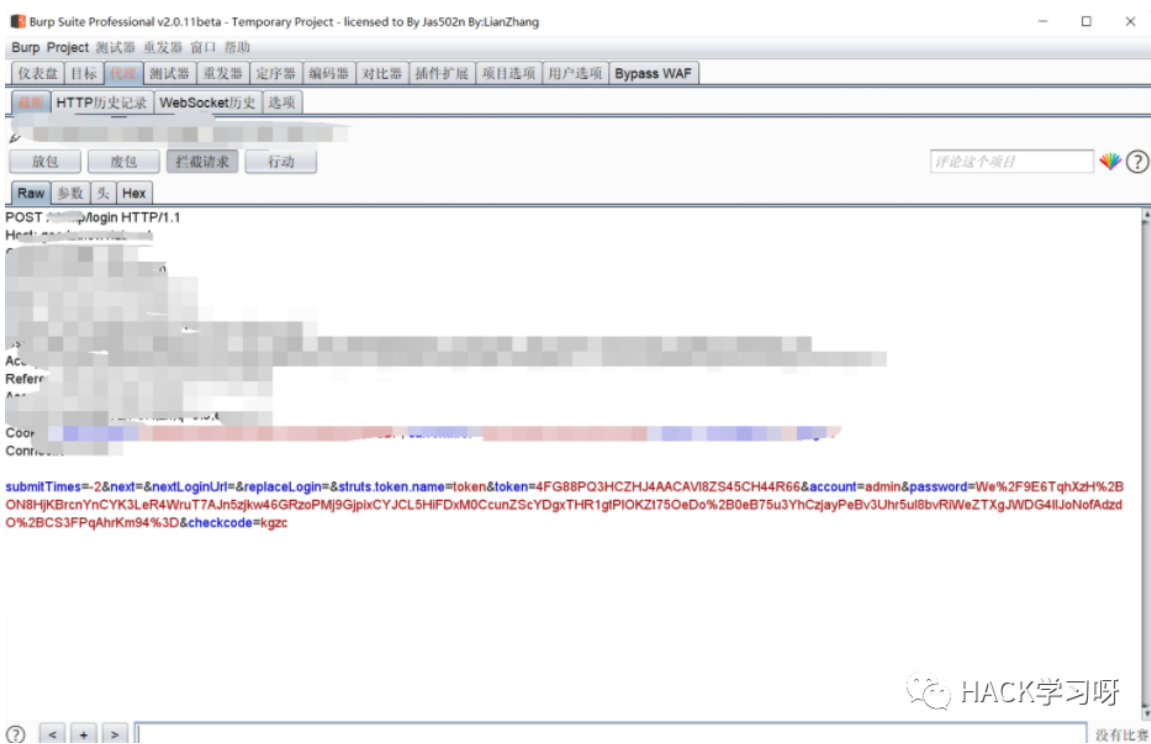
于是在这里抓包祭出神器BP



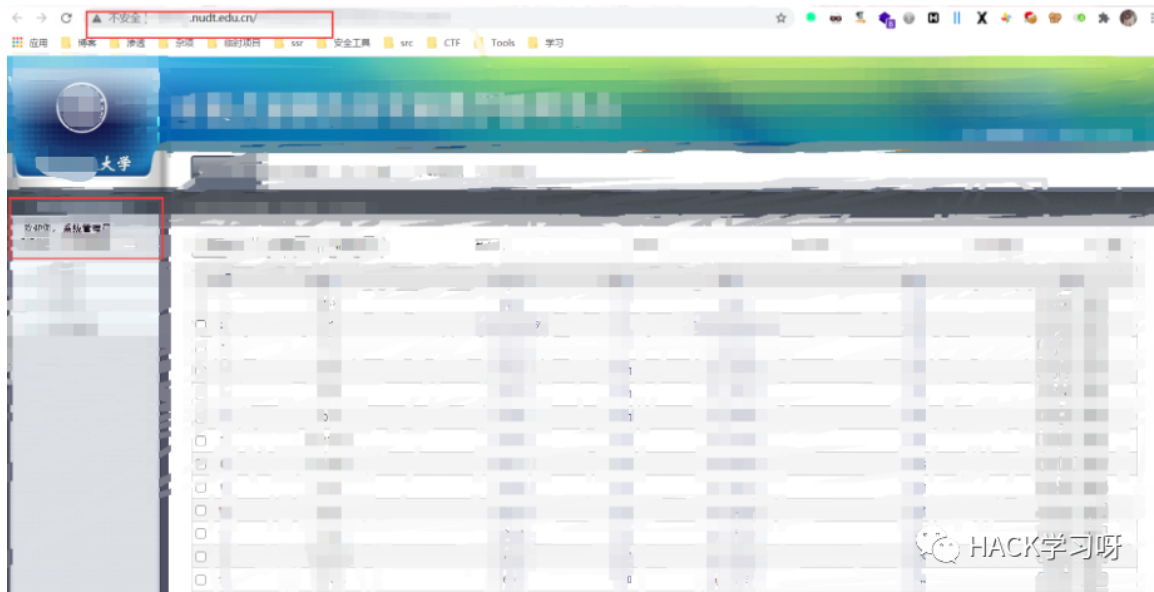
可以发现这里get方法传输了账户和密码 然后直觉和经验告诉我
直接把student改为admin



梭哈 这就进去了 后来发现这里不需要传 password 参数过去
也就是说只需要传一个用户名过去就能实现任意账户登录
然后这个系统正常的登录接口是



可以看出密码还是加密之后传进去 post 登录的
但是开发站的可能想着方便就放了一个登录测试账户的功能点 但是没有做任何限制
直接把管理员登录进去了



随便找了两个站截的图 现在已经修复了

然后就是fofa+google语法 批量梭哈



总共交了80多个站

几天就拿到了两个证书 美汁汁

订单列表

时间	商品	价格	发货
2021-01-03 18:29:43	漏洞报告证书-上海大学版	40	未发货
2021-01-03 11:45:59	原创漏洞报告证书-华南大学版	35	未发货

HACK学习呀




总结就是 仔细+运气



2021年性价比最高-网络安全系列课程

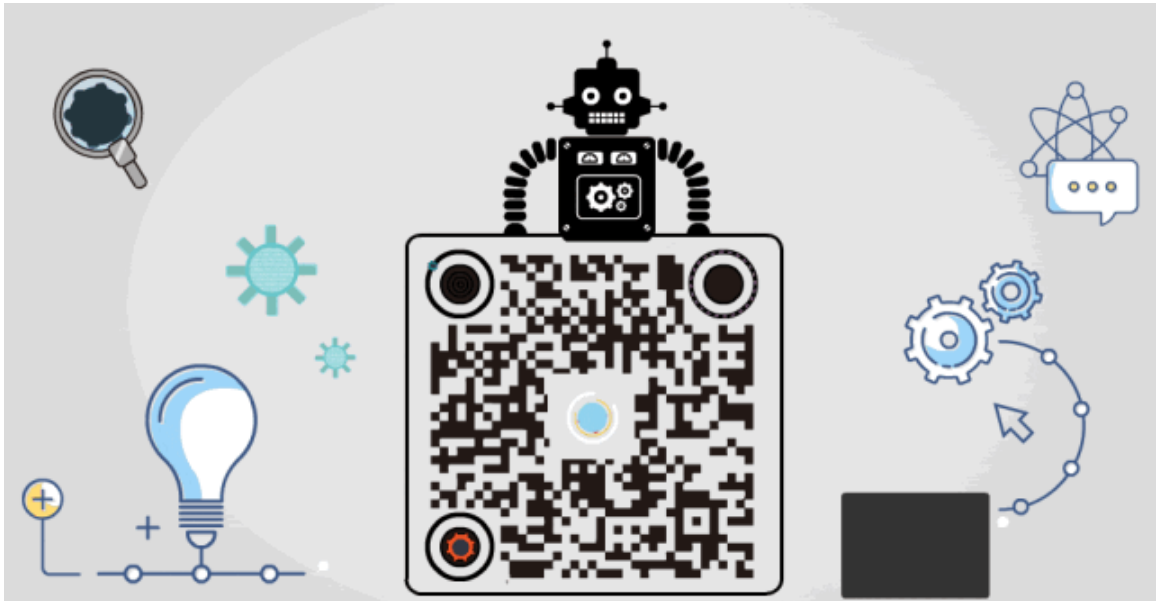
报名线上学习

从零开始学习白帽黑客

 HACK学习呀

点赞，转发，在看

原创投稿作者：Ma4ter



精选留言

用户设置不下载评论