逐鹿学院｜第六期带你走进一晚上30+漏洞的故事 课程总结>>

原创 兔安兔 Allsec安全服务平台 2022-05-17 19:07 发表于北京

收录于合集

#sql注入 4 #课程直播 4 #白帽子 4 #逐鹿学院 3

逐鹿学院第六期课程于2022年05月13日结束啦。本次课程是大家期待已久的漏洞分享，错过直播的小伙伴可以仔细阅读这篇文章，肯定会有您意想不到的收获哦。

01 课程信息

逐鹿学院第六期

讲师：Heart

课程内容：

- 拿到项目后如何快人一步
- 一个功能点竟有这么多漏洞
- 从未授权访问到任意修改数据
- 漏洞思路的无保留分享

参与人员：

课程面向对象为：Allsec安全服务平台安全专家，想要观看课程直播的小伙伴，需要先在平台官网：https://i.allsec.cn（点击阅读全文即可直接访问），进行账号注册哦，兔兔专门为你们准备了邀请码：
d15b56cc0a48441a927e94e1d680dc9c

02 课程内容回顾

拿到项目后如何快人一步

❖ 拿到项目后这样做：

刚拿到项目首先需要采集信息，但与挖掘src不同的是众测项目一般测试范围会有明确的规定，有的子域名可能不在测试范围内，所以一般都是直接采集项目测试范围内的信息。
大部分师傅测试可能就是使用各种目录扫描工具进行爆破，这样做不仅效率低而且还容易被禁用IP。

解决办法：
使用爬虫对网站进行爬取
推荐使用Radium和crawlergo
Radium下载地址：https://github.com/chaitin/rad
crawlergo下载地址：https://github.com/0Kee-Team/crawlergo

当然随着测试的深入，爬虫爬出来的信息肯定不满足于测试
这个时候我就会使用一款burp插件对js文件进行收集：BurpJSLinkFinder
工具下载地址：https://github.com/InitRoot/BurpJSLinkFinder
这个插件会自动整理好网站所有js文件中的一些链接目录等，在这里可以很容易发现一些未授权漏洞或者一些测试用的api接口。

既然提到了API安全方面，那么这里就再推荐一款API安全方面的burp插件
下载地址：https://github.com/API-Security/APIKit
APIKit可以主动、被动扫描发现应用泄露的API文档，并将API文档解析成BurpSuite中的数据包用于API安全测试。

❖ 总结

一：尽量不去爆破目录 ， 费时费力还容易被ban
选择爬虫爬取或者从js文件下手，仔细寻找可利用的url链接
例如：example.com/v3/info 访问403
在js文件里发现有/v1/user、/v2/admin
尝试使用/v1/：example.com/v1/info 访问200

二：在发现了未授权访问后，可以研究一些id等参数看是否存在sql注入漏洞

一个功能点竟有这么多漏洞

- 接口配置导致账号密码可爆破

由于正常的登录功能对密码的爆破可能会存在错误次数限制和验证码限制，那么我们可以通过修改密码时对原密码的检测来对原密码进行爆破。错误的就返回 0，并且没有验证码和速率限制，因此可以进行账号密码的爆破

- SQL注入漏洞

  由于修改密码这里会将我们输入的内容和数据库中的原密码进行校验，所以就有可能存在SQL注入漏洞。

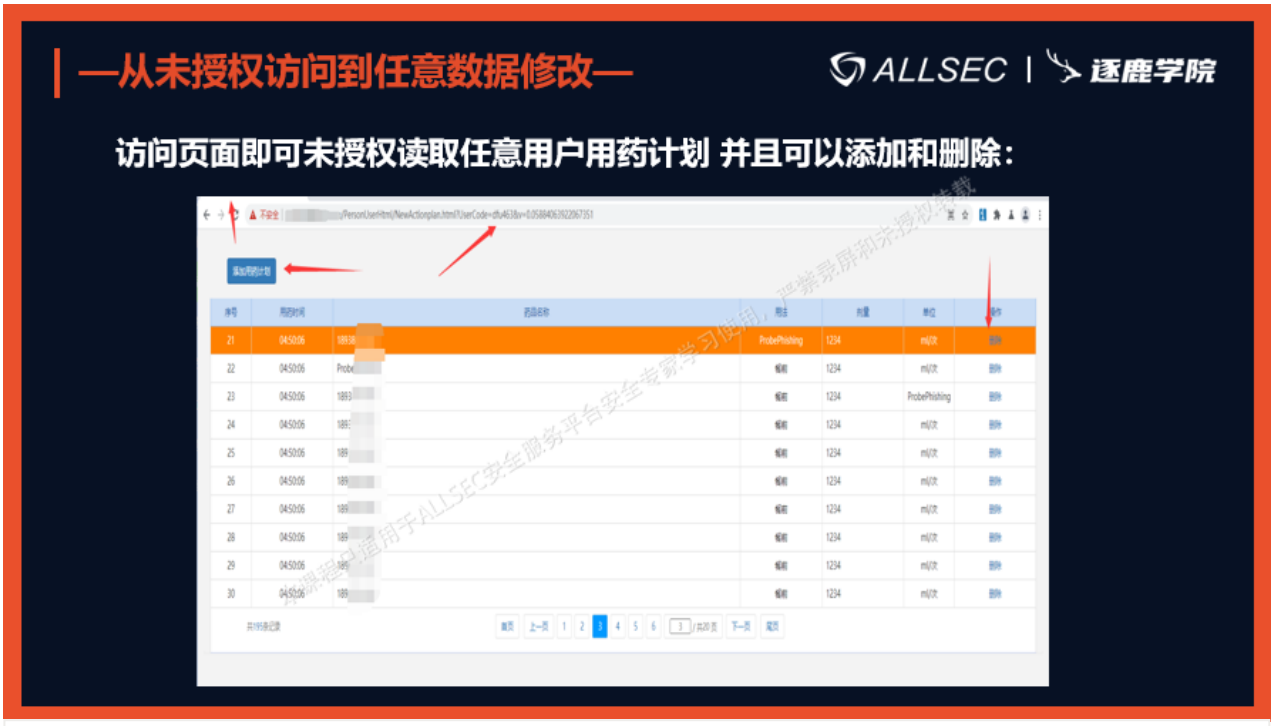
- 检测暗链工具

  在这里推荐一款好用的多线程暗链检测工具，方便大家对有问题的站点进行快速的检测，工具下载地址：

  https://github.com/heikanet/dc_find

从未授权访问到任意数据修改

访问页面即可未授权读取任意用户的“用药计划”信息并且可以添加和删除：



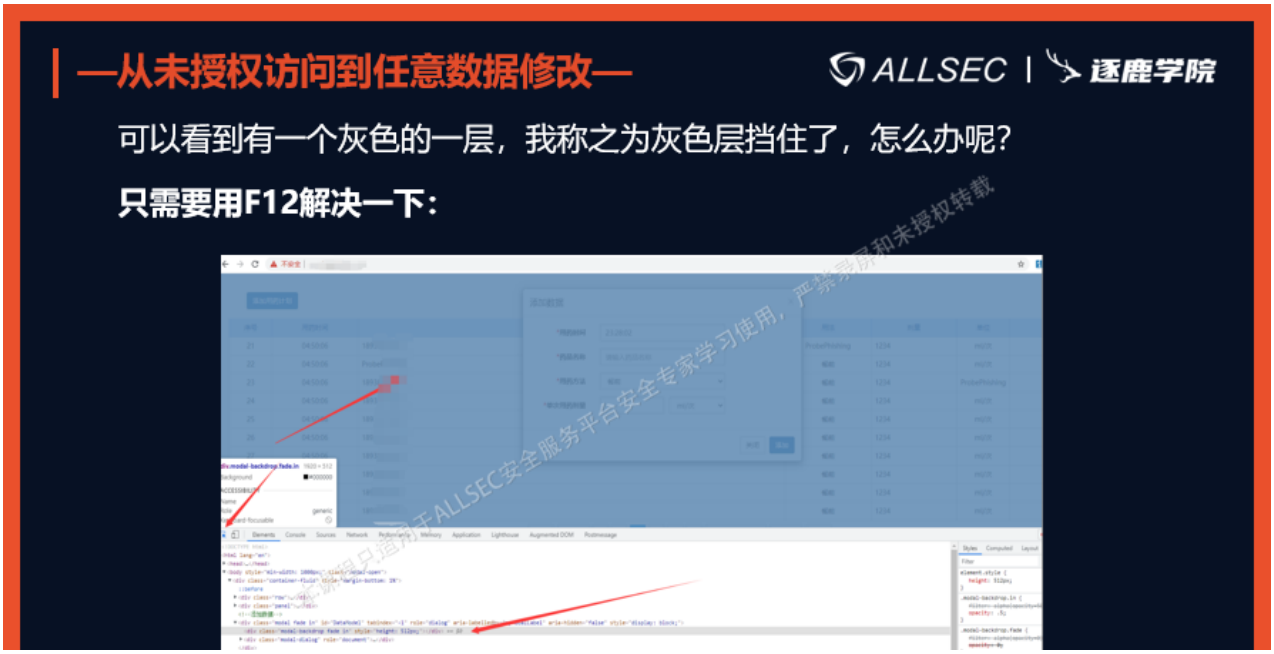
我们尝试查看“dfu307”用户的用药计划：

现在我们尝试添加和删除（自己注册的账号测试）

访问链接后点击“添加用药计划”功能，会出现以下情况

下图中可以看到“灰色层”挡住了功能点无法进行操作，怎么才能操作呢？

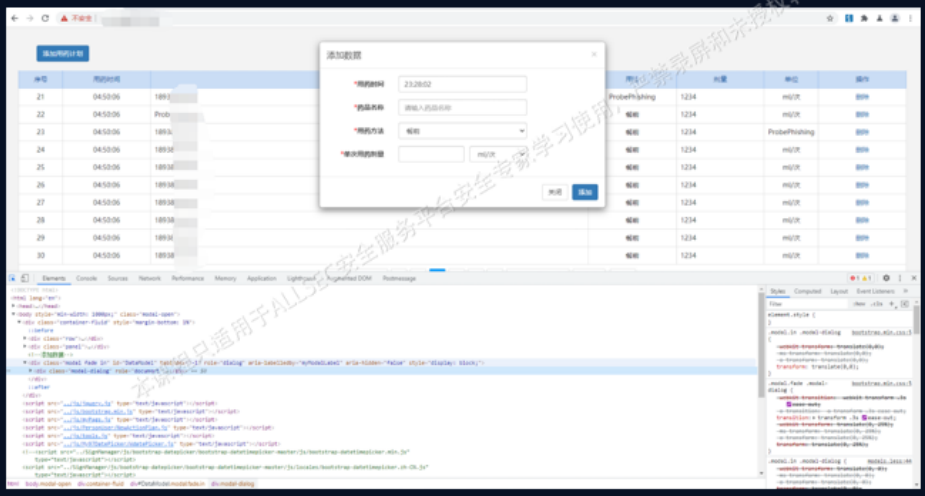
只需使用键盘上的“F12”解决。



—从未授权访问到任意数据修改—

ALLSEC | 逐鹿学院

用小箭头选中 然后找到代码后直接删除那一行 就可以删掉灰色层 如下：



漏洞思路的无保留分享

1.不受限的资源调用

idcard和truename参数代表身份证和姓名

当用户信息匹配的情况下certify_status返回“0”

—不受限的资源调用—

ALLSEC | 逐鹿学院

首先看到idcard和truename这两个参数 一看到这个链接就很有意思

那么当用户信息不匹配，会返回什么呢?

当用户信息不匹配的情况下certify_status返回“2”

下图中可以看到二要素认证接口的费用，漏洞不仅会被恶意利用，也会对企业资源进行消耗。

2.host碰撞工具

手工测试效率低且麻烦 那么这里我推荐个工具给大家

Hosts_scanV2优化版

下载地址：https://github.com/test502git/Hosts_scanV2

这个工具默认开启多线程模式（20线程），python3直接运行即可读取ip.txt和 hosts.txt遍历匹配访问。

03 课程直播反馈

是不是觉得本期课程干货满满呀，兔兔可全部为大家整理出来啦，接下来又回到课程问卷环节，本期课程安全专家的好评率达到了95%以上，快来看看还有哪些地方需要改进哦。

❖ 问卷建议

1、直播课是多久举办一次，能不能多来几期？

回复：感谢对此次课程的肯定，逐鹿学院课程会定期开课，也会不断更新迭代的，敬请期待~

2、PPT可以分享一下吗？有录播吗？

回复：因为本次课程是为平台用户打造的非公开课程，所以ppt和视频暂不对外公布，不过课程结束后我们会在公众号发布课程总结哦，也可以帮助您进行学习的。

3、课程节奏快，有点来不及记笔记。

回复：课程的笔记兔兔都帮大家整理好啦，这篇文章里都有哒。

……

❖ 下期免门票参与人员

bbw、Rarry、NOBFS_、Rue、The丶Lost 、小羊丢了在找羊、无名草、冬夏、Npce3r、APCE

兔兔再次提醒大家，课程结束后参与问卷调查有机会免门票参与下一期逐鹿学院课堂，或者转发此篇文章同样也是有机会免门票参与下一期课程哒，可不要错过每一期免门票参与课程的机会哦。

另外逐鹿学院讲师持续招募中，感兴趣的小伙伴可以私聊兔兔哦。

积分大放送，推荐别人入职，您就能获得奖励

1.推荐实习岗位成功入职且通过试用期，奖励200积分

2.推荐初级渗透测试工程师成功入职且通过试用期，奖励300积分

3.推荐中级渗透测试工程师成功入职且通过试用期，奖励600积分

4.推荐高级渗透测试工程师成功入职且通过试用期，奖励1000积分

有任何疑问可微信扫码联系兔安兔 ~

Allsec安全服务平台

Allsec众测平台官方账号，发布众测最新活动，构建众测生态，增强企业网络安全行业...

11篇原创内容

公众号

阅读原文

喜欢此内容的人还喜欢

逐鹿学院第六期｜带你走进一晚上漏洞30+的故事!

Allsec安全服务平台