NUC WEB Write-Up

首先御剑扫一下，看看有没有敏感目录泄漏。发现了robots.txt，里面有一个目录ciscnshopheart，但直接访问发现还是是一个sshop，猜测是做了路由，加上index.php，发现是一个购物心得体会记录系统，再看看有没文件泄漏，扫描后发现了api.php.swp common.php.swp riji.php.swp

在common.php中看到了foreach和$$key的组合，如果变量没有进行初始化，那么我们可以初始化该变量。早riji.php中找到了一个没有初始化的变量，登陆后，session就会保存，所以第一个判断可以进入，如果登陆了一个用户后在删除这个用户，那么就不会存在这个用户的id，我们就可以将userid覆盖。

第二个变量在api.php中，这个需要反序列化的api没有经过初始化，所以我们同样可以覆盖导致反序列化的漏洞。在riji.php中，发现了使用id进行查询，id可以进行变量覆盖

经过以上分析，我们现在登陆一个用户，反序列化一个del_user的方法将其删除，最后覆盖id变量进行注入

在审计del_user方法，需要check==1,也就是管理员可以删除。而管理员检查时通过salt加上用户名进行md5加密的。但username要校验为admin，只要知道salt的md5就可以绕过

在找回密码处审计有一个302跳转，可通过forget页面获取check中的salt的加密值，接着利用md5扩展攻击获取admin的加盐hash

至此，我们就可以在查询日记处进行常规的sql注入了，id=-1 union select 1,2,flag from flag