XCTF 攻防世界 Web题的基本知识点

原创

sherlockjjobs 于 2020-11-28 13:47:30 发布 1947 收藏 3

分类专栏： CTF Web

本文链接：https://blog.csdn.net/weixin_43456810/article/details/110261950

XCTF 攻防世界 Web题的基本知识点和解题思路

1. 大多数情况下，robots协议指的就是robots.txt
2. index.php的备份文件：/index.php.bak
3. 页面中如果出现了不能按的按钮，可能是代码中设置了disable参数，将网页源代码中的disable=""删除或者改为false（注意：safari浏览器可能无法方便的直接修改源代码，可以换为firefox浏览器）
4. 遇到php的源代码，注重分析，如果只是简短的几行代码，并且有类似于$a, $b这样的变量，可以直接在url的后面添加上 /?a=…&b=…进行尝试
5. 如果题目中要求用GET方法发送一个值时，可以直接在url的后面添加 /?a=…（如果是POST方法，firefox浏览器使用hackbar插件可以很容易的解决；当然，利用burpsuite拦截发包也是可以的，注意：在用burpsuite进行POST请求的时候，需要加上Content-Type: application/x-www-form-urlencoded)
6. X-Forwarded-For和Referer是很重要的两个参数，用于请求的伪造。如果题目中一定要某个ip地址的话，可以使用X-Forwarded-For参数指定ip地址，如X-Forwarded-For: 127.0.0.1; Referer参数用于伪造来源，如Referer: https://www.baidu.com
7. 题目中出现了一句话木马，如<?php @eval($_POST['shell']); ?>，则可以尝试用蚁剑(AntSword)进行连接，连接密码即为shell
8. 命令执行漏洞通常是由于没有WAF，如经常出现的ping命令，可以在输入框中尝试 ping 127.0.0.1 | find / -name “flag”，利用连接管道符可以显示多条命令执行的结果
9. 题目中出现了\x这样的16进制，可以先尝试将16进制转为10进制，再转为相应的ASCII码
10. 如果知道了php的版本，则进行搜索此版本对应的漏洞，找到利用漏洞PoC代码，进行尝试
11. 看到php代码中有类似$ page的变量以及include($page)这样的语句，可以尝试构造 /?page=php://input 伪协议，如果php代码中有strstr区分大小写的函数)，通过直接大小写，/?page=PhP://input绕过
12. 在题目的网页中（如index.php页面），发现后面有id=1这样的形式，在暂时尝试了其他方法无果或者没有思路的情况下，可以尝试暴力破解。经常使用burpsuite的Intruder模块进行暴力破解，选择payload或者导入字典
13. 如果题目页面中只有一张图片的话，查看网页的源代码，寻找信息，在源代码中可能隐含flag的文件信息，如hint.php, flag.php，然后在url的最后添加?file=hint.php进行尝试
14. 看到搜索框，首先想到的肯定是SQL注入和XSS注入，SQL测试：通常先输入1，看看有没有返回值；XSS测试：输入“><script>alert(1)< /script><”，看有没有回显的框弹出。如果确定为是SQL注入，可以尝试进行手动注入（一步一步的进行深入）；也可以拦截抓包进行POST请求，然后将请求保存为request.txt文件（文件名随意取），通过自动化工具sqlmap进行自动注入：sqlmap -r request.txt --dbs，在发现了数据库的名称之后，可以尝试 sqlmap -r request.txt -D 数据库名 --dump，

直接将数据库的内容都dump出来。（注意：在实际的操作中，很少有完全借助sqlmap进行注入的情况，通常都是手动注入和sqlmap相结合）

15. 遇到打不开的网页时，可以将后缀名改为html，尝试打开
16. 如果题目中的script代码的最后是eval(_)，将eval改为alert，在回显之后的代码里寻找和flag相关的，如正则表达式，放在控制台里运行一下，可能会看到flag的信息
17. 在php代码里，__代表魔术方法，如果php代码中出现了__wakeup()方法，则可能跟php的序列化和反序列化相关。反序列化，首先要序列化。如果代码足够简单，则可以在代码最后加上 $a=new 类名(); echo(serialize($a)); 将序列化的结果显示出来。要绕过__wakeup()方法，可以将序列化字符串中的对象个数修改一下，最后将反序列化的结果添加到url的最后
18. 遇到文件上传漏洞的题目，可以先准备准备一句话木马上传，如<?php highlight_file(_FILE_); system($_GET['cmd']); ?>。上传的文件首先可以尝试更改文件名，如1.php.jpg，如果不行，则可以在上传的同时，利用burpsuite拦截抓包，将文件名更改一下，大多数情况下就可以绕过过滤。上传成功后，则可以在request请求的最后（与http头的参数隔一行）加上 <?php system('ls'); ?>，继续send，会看到显示的目录，通过更改命令一步步的深入，获取flag信息
19. 查看php源文件的话，可以在最后加上s，也可以在url的最前面加上view-source:（注意：safari中时无法使用view-source显示源代码的，要使用firefox）
20. python模块注入的问题，首先在url的最后加上 /{{7+7}} 进行判断，如果页面中显示了相加的和，则说明存在服务器模版注入(SSTI)，在url的最后添加 /{{config.items()}}，显示出所有变量的信息，然后构造 `{{''.__class__.__mro__[2].__subclasses__()[59].__init__.func_globals.linecache.os.popen('ls').read()}}`，看到flag信息后，继续构造 `{{''.__class__.__mro__[2].__subclasses__()[59].__init__.func_globals.linecache.os.popen('cat fl4g').read()}}`，就可以获取到flag了