LINUX平台上一种WEB漏洞灰盒测试方法

Shellshock漏洞

Apache服务器使用mod_cgi或者mod_cgid，如果CGI脚本在BASH或者运行在子SHELL里都会受影响。子Shell中使用C的system/popen，Python中使用os.system/os.popen，PHP中使用system/exec(CGI模式)和Perl中使用open/system的情况都会受此漏洞影响。

对于perl的system函数

execvp()函数

元字符

Symbol	Meaning
>	Output redirection
>>	Output redirection (append)
<	Input redirection
*	File substitution wildcard; zero or more characters
?	File substitution wildcard; one character
[ ]	File substitution wildcard; any character between brackets
`cmd`	*Command Substitution*
$(cmd)	*Command Substitution*
|	*The Pipe (|)*
;	Command sequence, *Sequences of Commands*
||	OR conditional execution
&&	AND conditional execution
( )	Group commands, *Sequences of Commands*
&	Run command in the background, *Background Process*
#	Comment
$	Expand the value of a variable
\	Prevent or escape interpretation of the next character
<<	Input redirection (see *Here Documents*)

对于perl的system函数

```
!#/usr/bin/perl
 system(“id”);

 !#/usr/bin/perl
 $url=“$”;
 system(“wget $url”);

 !#/usr/bin/perl
 $url=“$”
 system(“wget”,$url);
```

audit

audit是linux系统中用于记录用户底层调用情况的系统，如记录用户执行的open,exit等系统调用。并会将记录写到日志文件中。

audit可以通过使用auditctl命令来添加或删除audit规则。设置针对某个用户进行记录，或针对某个进程的进行记录。

audit安装

- 安装：yum install audit
- 启动：service auditd start
- 配置: /etc/audit/auditd.conf
  max_log_file = 5 (兆)

audit使用

服务状态

auditctl -s

添加规则

auditctl -a entry,always -F uid=500

查看已有规则

auditctl -l

测试思路

监控 auditd.log寻找调用bash的时间

转化调用bash的时间戳为本地时间查找access_log找出对应的url

对url进行实际测试

演示

拓展

寻找命令注入
查找后门

。。。。。。。。。。