

Shellshock 攻击

版权所有 © 2017 作者：杜文亮，保留所有权利。

允许个人使用。利用这些问题只有当作者的书被采用作为该课程的教科书时，该课程才被授予。所有其他用途必须征得作者同意。

W6.1. 如果把一个含有 shell 函数定义的 shell 变量作为环境变量传递给子进程，该函数定义会发生什么？

W6.2. 假设父 Bash 定义并导出了一个 shell 函数，随后启动一个同样运行 Bash 的子进程。请解释父 Bash 中的函数如何成为子 Bash 中的函数。

W6.3. 编写一个试图利用 Shellshock 漏洞的 Bash 函数定义。

W6.4. 如果不把额外的 shell 命令放在函数定义之后，而是放在定义之前（如下所示），再启动存在 Shellshock 漏洞的 Bash，命令 `echo world` 会执行吗？

```
$ export foo='echo world; () { echo hello;}'  
$ bash
```

W6.5. 要利用 Shellshock 漏洞，需要满足哪两个条件？

W6.6. 用户输入是如何以环境变量的形式进入远程 Bash CGI 程序的？

W6.7. 对 CGI 程序实施 Shellshock 攻击时，能否不使用函数定义，而直接把 shell 命令放入 `User-Agent` 字段，使 Bash 启动后执行该命令？

W6.8. ★

Shellshock 漏洞为什么会出现？可以从中吸取什么教训？

W6.9. 还可以通过把输入附加在 URL 后面来向 CGI 程序传递数据，例如：

```
http://www.example.com/myprog.cgi?name=value
```

能否把恶意函数定义放入上述 URL 的 `value` 字段，使其进入该 CGI 程序的环境变量并触发 Shellshock？

W6.10. 在机器 1（IP 地址为 10.0.2.6）上运行 `"nc -l 7070"`，随后在机器 2 上输入以下命令。将会发生什么？

```
$ /bin/cat < /dev/tcp/10.0.2.6/7070 >&0
```

W6.11. 如何在机器 1 上运行 `/bin/cat`，使它从机器 2 读取输入，并把输出发送到机器 3？

W6.12. 考虑以下程序：

```
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

extern char **environ;

int main()
{
    char *args[] =
    {
        "/bin/sh", "-c",
        "/bin/ls", NULL
    };
    pid_t pid = fork();

    if(pid == 0) {
        /* child */
        printf("child\n");
        execve(args[0], &args[0], NULL); ①
    }
    else if(pid > 0) {
        /* parent */
        printf("parent\n");
    }
    return 0;
}
```

程序创建一个子进程，并通过 `/bin/sh` 执行 `/bin/ls`；这里 `/bin/sh` 是指向 `/bin/bash` 的符号链接。按如下方式运行程序，请说明输出及其原因。

```
$ gcc prog.c -o prog
$ export foo='() { echo hello; }; echo world; '
$ ./prog
```

W6.13. 把问题 W6.12. 中第 ① 行改为以下代码，然后重新回答该题。

```
execve(args[0], &args[0], environ);
```

W6.14. 考虑一个作为 Apache 模块运行的 PHP 程序和一个 CGI 程序。

PHP 程序 (test.php):

```
<?php
    system("/bin/ls -l")
?>
```

CGI 程序 (test.cgi):

```
#!/bin/sh
/bin/ls -l
```

两个程序都会在新的 shell 进程中调用 `/bin/ls` (`/bin/sh` 指向 `/bin/bash`)。按如下方式访问它们时, Shellshock 对两种情况的影响有何不同? 各自需要满足什么条件才能利用漏洞?

```
$ curl -A "()" { echo hello; }; echo world;" http://localhost/test.php
$ curl -A "()" { echo hello; }; echo world;" http://localhost/test.cgi
```