命令注入攻击实战

1. Low 级别命令注入攻击实战

步骤 1：安全级别设置为 low，点击 Command Injection 按钮，进入命令注入攻击页面，发现是一个 Ping 命令执行页面，在文本框中输入一个 IP 地址或者域名，页面会返回 Ping 的结果，如图 1.1。

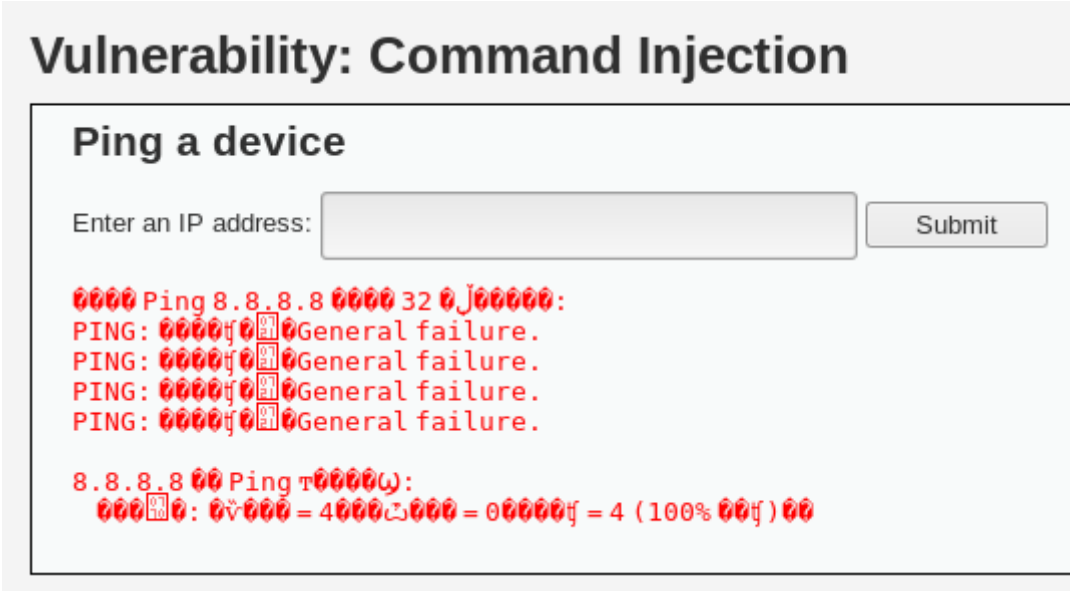

图 1.1

步骤 2：由于本服务器使用的是 Windows Server 系统，所以我们可以使用 Windows 的系统命令来进行注入攻击。在文本框中直接输入 net use 命令，发现报错，如图 1.2，说明页面会把文本框中提交的信息提交为 Ping 的参数来执行。

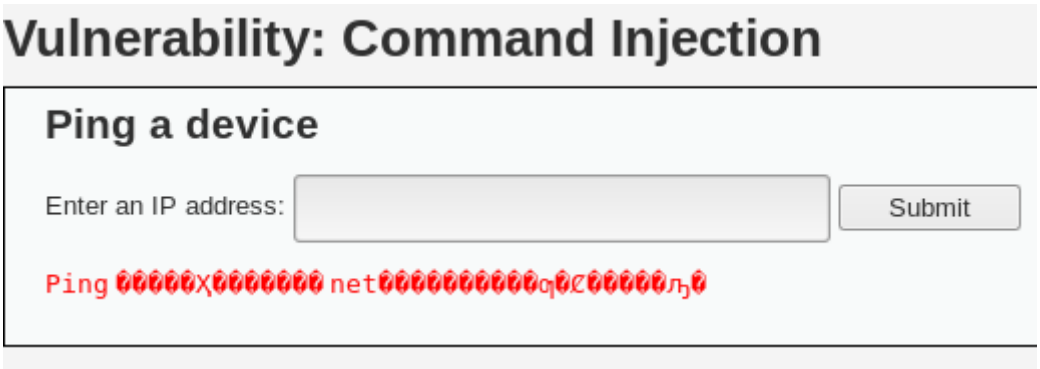

图 1.2

步骤 3：Windows 系统和 Linux 系统都可以使用 && 符号来连接多条命

令，从而一次执行。所以我们尝试在文本框中先输入一个正确的 IP 地址，再用 && 符号来连接另外一个命令。输入 192.168.119.100&&net user，发现成功注入，页面返回 net user 命令的执行结果，如图 1.3。

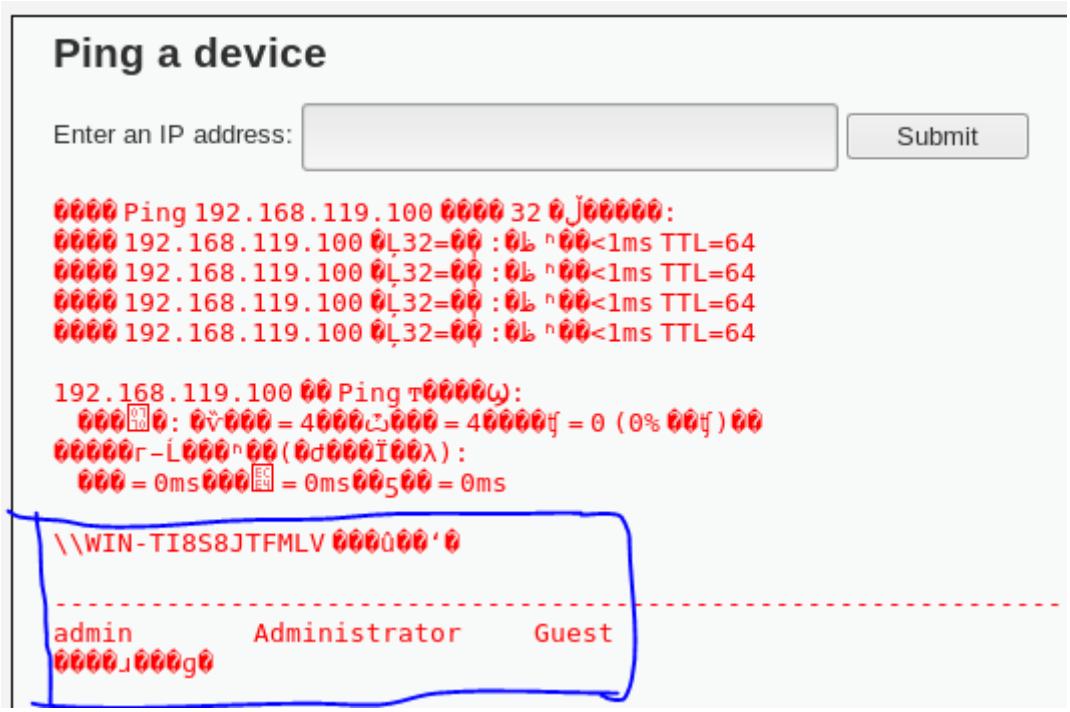

图 1.3

2. Medium 级别命令注入攻击实战

步骤 1：设置安全级别为 Medium，进入命令注入攻击页面，查看页面源码，发现对 && 和 ；进行了过滤，转换为空值，如图 2.1。

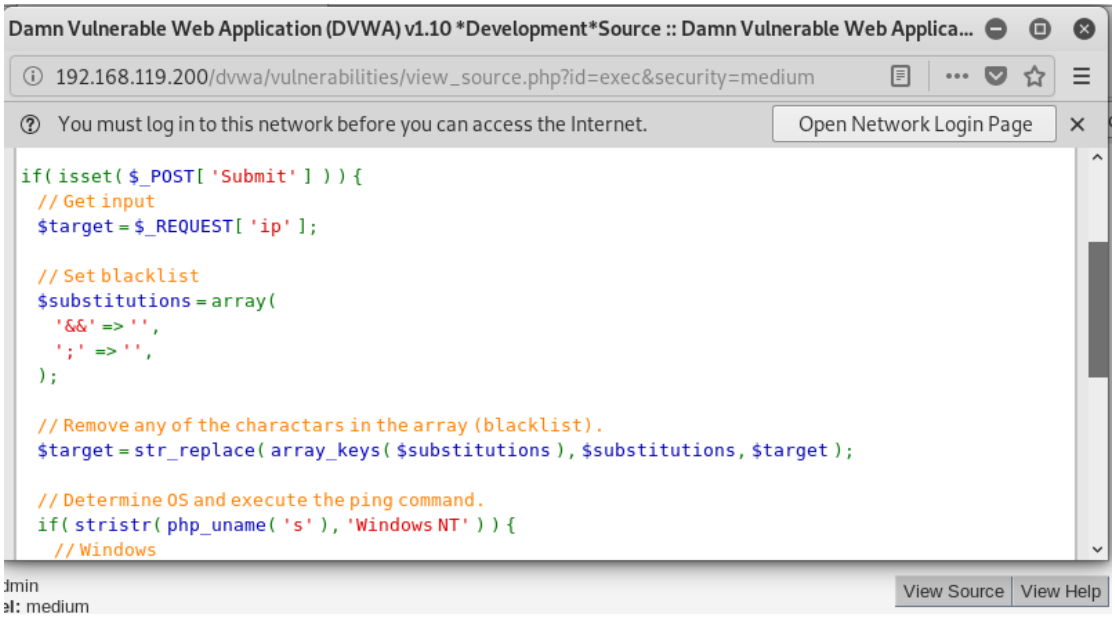

图 2.1

步骤 2：页面只是过滤了 && 和 ;，但是并没有对单 & 符号进行过滤。在文本框中输入 192.168.119.100&net user，发现可以绕过防御成功注入，如图 2.2。

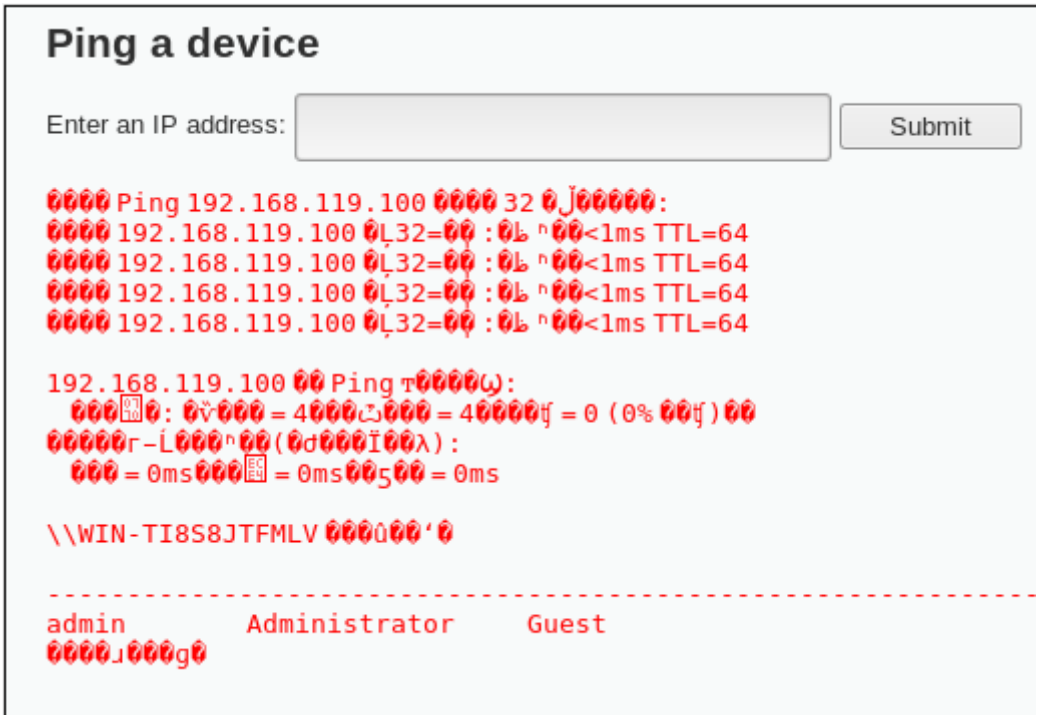

图 2.2

&& 和 & 的区别是，&& 是只有当前一个命令执行成功后，才会执行第二个命令；而 & 是不管第一个命令是否执行成功，都会执行第二个命令。

3. High 级别命令注入攻击实战

步骤 1：设置安全级别为 High，进入命令注入攻击页面，查看页面源码，发现几乎对所有命令连接符都做了过滤，如图 3.1.

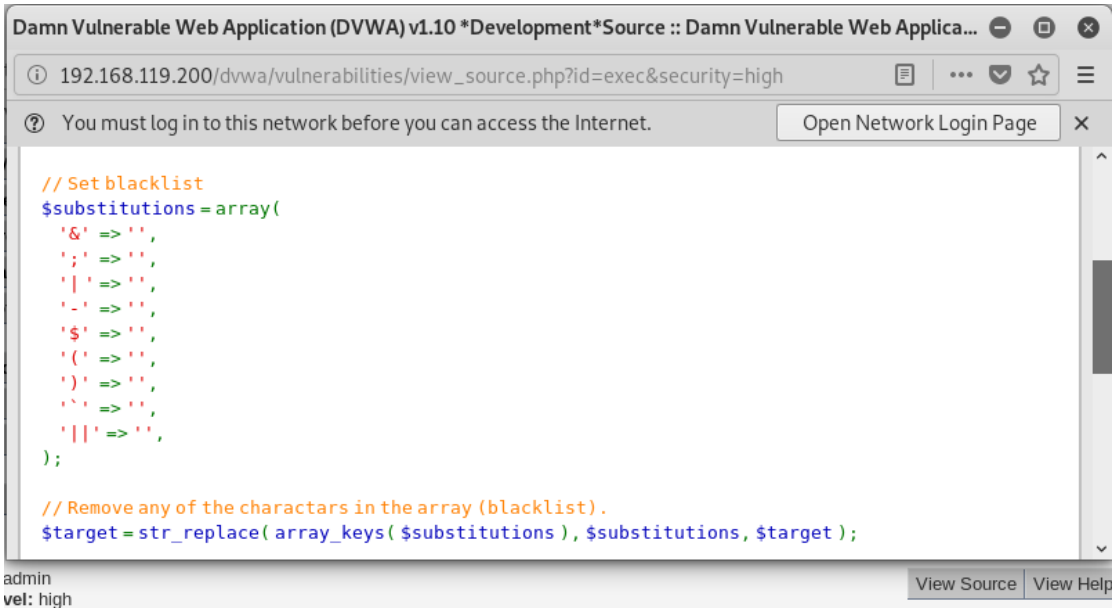

图 3.1

步骤 2：继续观察页面源码，发现对 | 管道符的过滤中，管道符后有一个空格，如图 13-6。由于过滤不严谨，使得 | 符有了可趁之机。在文本框中输入 192.168.119.100|net user，可以成功注入，如图 3.2。

图 3.2