PhpStudy 后门复现以及检测

2019 年 10 月 23 日

11:27

1.1. 软件说明：

phpStudy 是一个 PHP 调试环境的程序集成包。该程序包集成最新的 Apache+PHP+MySQL+phpMyAdmin+ZendOptimizer，一次性安装，无须配置即可使用，是非常方便、好用的 PHP 调试环境。该程序不仅包括 PHP 调试环境，还包括了开发工具、开发手册等。在“杭州警方通报打击涉网违法犯罪暨“净网 2019”专项行动战果”的文章中，说明了一些网站下载的 phpstudy 版本中存在后门。数十万安装用户成为肉鸡。

1.1.1. 漏洞验证：

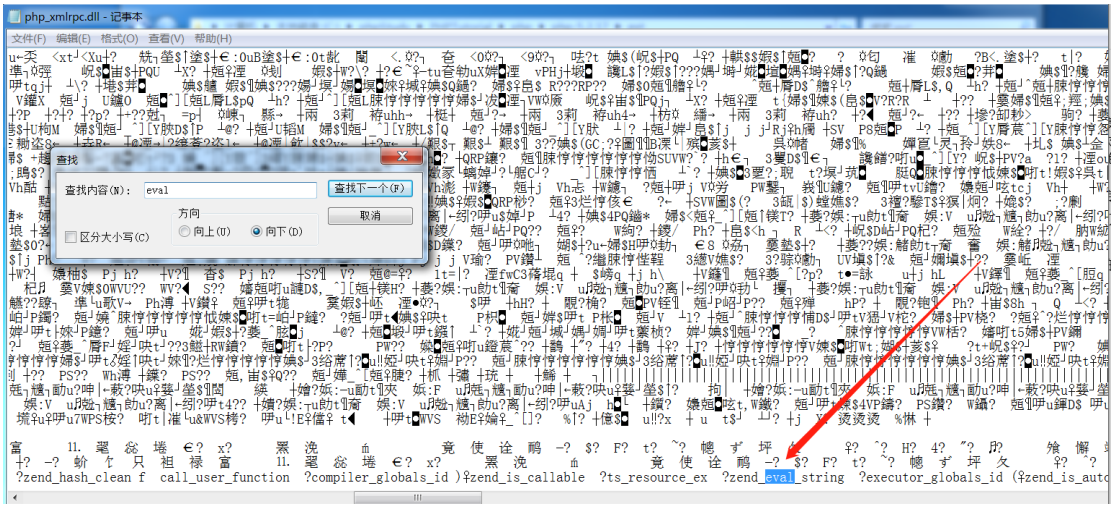
存在后门的 phpStudy 版本为 2016 和 2018 版本。在安装的 php 目录下
存在版本的 php 文件为：
Php-5.2.17
Php-5.4.45

1.1.2. 文件路径为：

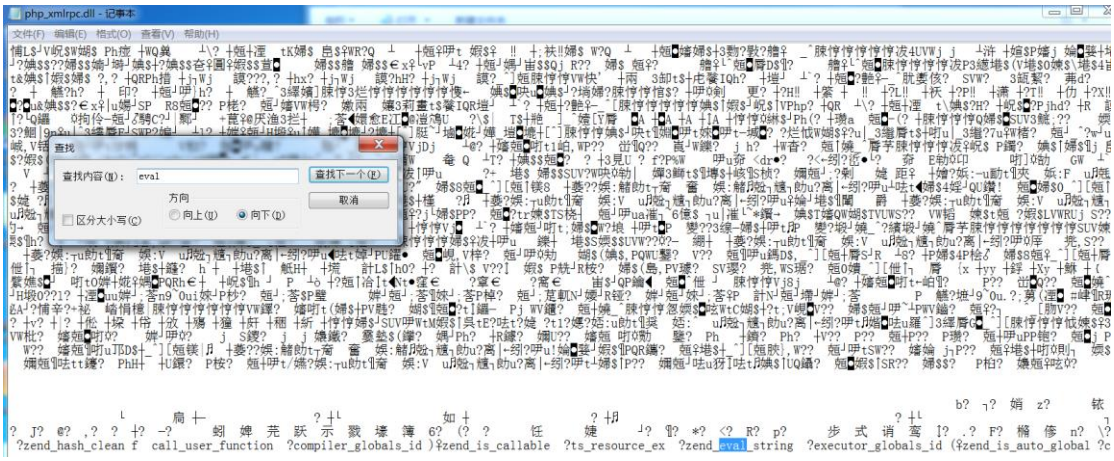
php\php-5.2.17\ext\php_xmlrpc.dll
php\php-5.4.45\ext\php_xmlrpc.dll

1.1.3. 判断是否存在漏洞：

5.2.17



5.4.45



1.2. 漏洞利用：

安装完 phpStudy 后，访问

通过 burpsuit 抓取数据包，添加 payload,这里，需要更改数据包内容

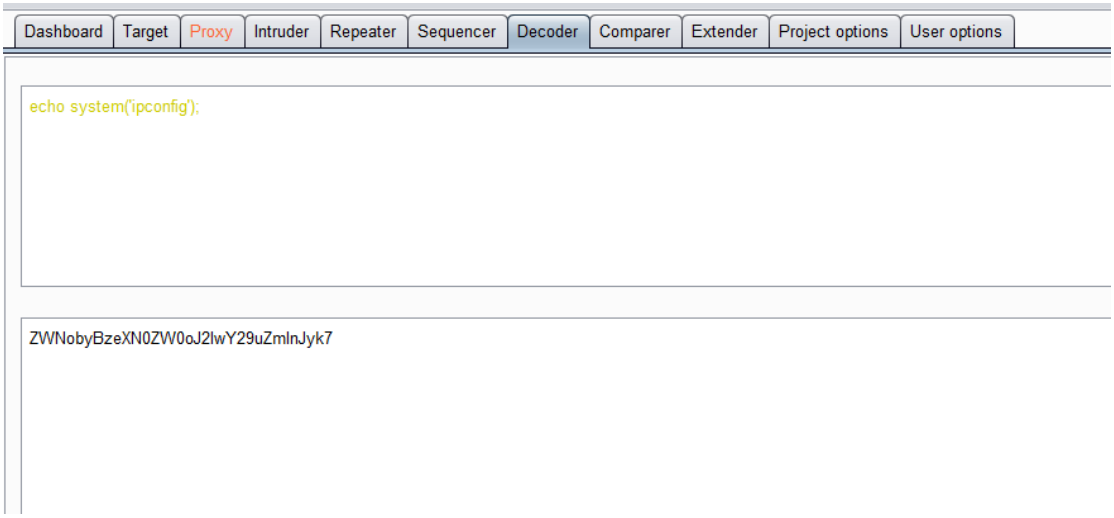
1.2.1. 添加：

在数据包中添加以下内容

Accept-Charset: ZWNobyBzeXN0ZW0oJ2lwY29uZmlnJyk7

其中 ZWNobyBzeXN0ZW0oJ2lwY29uZmlnJyk7 为所执行命令的 base64 编码

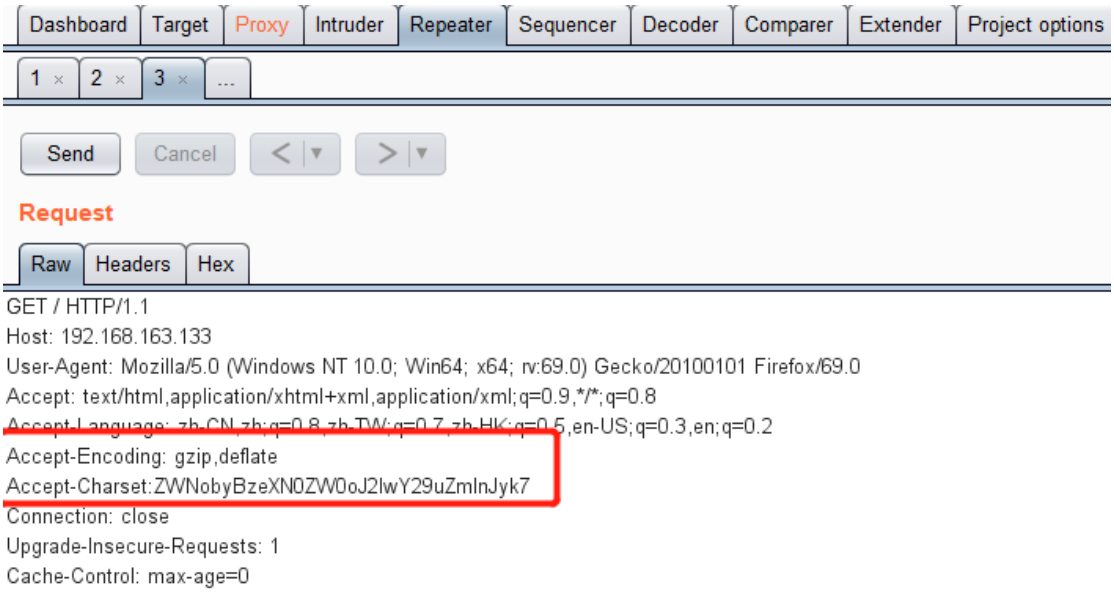
Base64 执行代码



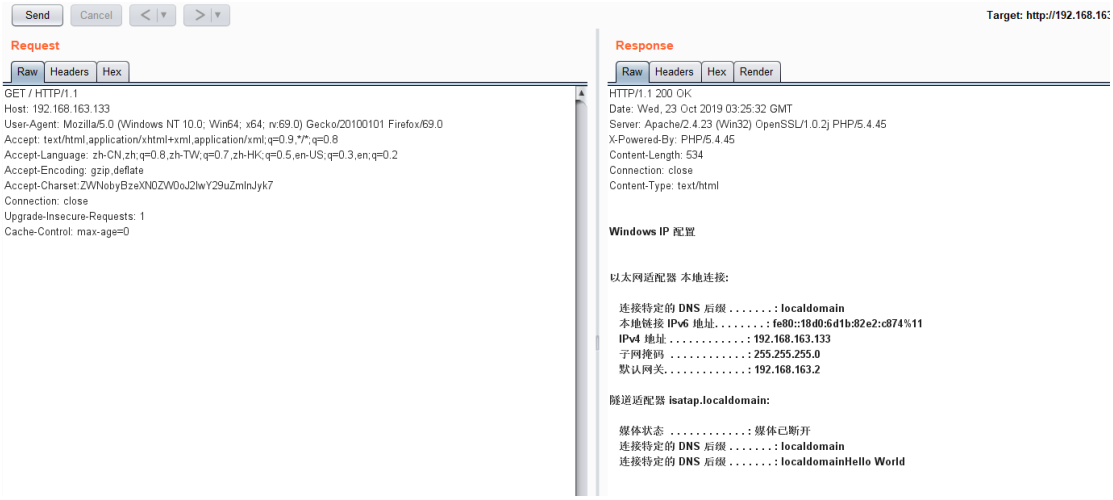
1.2.2. 删除：

要删除数据包中的 Accept-Encoding: gzip, deflate 中 gzip 后面的空格

Accept-Encoding: gzip,deflate



放行数据包，可得命令执行的回显信息



1.3. 缓解：

目前，绝大部分得下载站都更新了 phpStudy 安装包，带有漏洞得版本很难找到，验证方法很简单，也就是 dll 中的关键字 eval.要想避免下载漏洞版本的软件，建议到官网下载，不要在下载站中下载来源不明的软件安装包。