

CTF爆破

原创

Skn1fe 于 2021-02-24 20:04:26 发布 413 收藏 1

文章标签: [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_45086218/article/details/114028156

版权

文章目录

[Authorization认证](#)

[域名爆破](#)

[md5爆破](#)

[伪随机数](#)

[php_mt_seed 爆破](#)

[目录爆破](#)

本文以ctf.show网站题目为例, 总结ctf中的爆破姿势

Authorization认证

登录以访问此站点

http://f8541d76-64c9-4abb-a5da-eb24f55cd7dd.chall.ctf.show:8080 要求进行身份验证
与此站点的连接不安全

用户名

密码

登录

取消

https://blog.csdn.net/qq_45086218

Request

Raw Headers Hex

```
GET / HTTP/1.1
Host: f8541d76-64c9-4abb-a5da-eb24f55cd7dd.chall.ctf.show:8080
Cache-Control: max-age=0
Authorization: Basic YWRtaW46MQ==
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36 Edg/88.0.705.74
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://f8541d76-64c9-4abb-a5da-eb24f55cd7dd.chall.ctf.show:8080/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6
Connection: close
```

Response

Raw Headers Hex Render

```
HTTP/1.1 401 Unauthorized
Content-Type: text/html; charset=utf-8
Date: Wed, 24 Feb 2021 09:02:08 GMT
Server: nginx/1.16.1
Www-Authenticate: Basic realm="è-è%0à0#adminç00ç0"æ0·â00â00â0ç 0"
X-Powered-By: PHP/7.3.11
Connection: close
Content-Length: 42
```

需要用户名和密码才能继续访问

https://blog.csdn.net/qq_45086218

Base64 编码或解码的结果:

admin:1

基于这一点进行爆破

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Va and each payload type can be customized in different ways.

Payload set: 1 Payload count: 4,451

Payload type: Simple list Request count: 4,451

? Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Add Add from list ...

!@#%&^* \$\$\$\$ *****575783. 0000 00000

Enter a new item

? Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Edit Remove Up Down

Enabled	Rule
<input checked="" type="checkbox"/>	Add Prefix: admin:
<input checked="" type="checkbox"/>	Base64-encode

? Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: .\=\<>?+&*;"'[]|^\`

https://blog.csdn.net/qq_45086218

域名爆破

二级域名挖掘

或通过BP爆破子域名:

*.ctfer.com

md5爆破

```
include('flag.php');
if(isset($_GET['token'])){
    $token = md5($_GET['token']);
    if(substr($token, 1,1)===substr($token, 14,1) && substr($token, 14,1) ===substr($token, 17,1)){
        if((intval(substr($token, 1,1))+intval(substr($token, 14,1))+substr($token, 17,1))/substr($token, 1,1)===intval(substr($token, 31,1))){
            echo $flag;
        }
    }
}
}else{
    highlight_file(__FILE__);
}
}
```

https://blog.csdn.net/qq_45086218

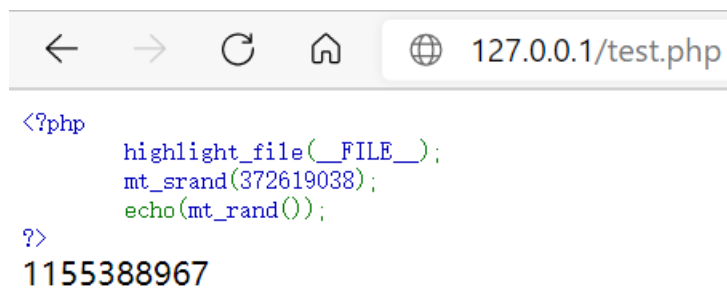
```
<?php
error_reporting(0);

$a="asdfghjklqwertyuiopzxcvbnm1234567890";
for($i=0;$i<36;$i++){
    for($j=0;$j<36;$j++){
        $token=$a[$i].$a[$j];
        $token = md5($token);
        if(substr($token, 1,1)===substr($token, 14,1) && substr($token, 14,1) ===substr($token, 17,1)){
            if((intval(substr($token, 1,1))+intval(substr($token, 14,1))+substr($token, 17,1))/substr($token, 1,
1)===intval(substr($token, 31,1))){
                echo $a[$i].$a[$j];
                exit(0);
            }
        }
    }
}
?>
```

伪随机数

```
error_reporting(0);
include("flag.php");
if(isset($_GET['r'])){
    $r = $_GET['r'];
    mt_srand(372619038);
    if(intval($r)==intval(mt_rand())){
        echo $flag;
    }
}else{
    highlight_file(__FILE__);
    echo system('cat /proc/version');
}
```

每一次mt_rand()被调用都会根据seed和当前调用的次数i来计算出一个伪随机数
可以用srand()或mt_srand()给随机数发生器播种
所以其实mt_rand是定值



php_mt_seed 爆破

```
sudo ./php_mt_seed 伪随机数
```

```
sknife@kali:~/php_mt_seed$ sudo ./php_mt_seed 597367078
Found 0, trying 973078528 - 1006632959, speed 143099783 seeds per second
Found 0, trying 1006632960 - 1040187391, speed 142987636 seeds per second
seed = 1036634921
Found 1, trying 1040187392 - 1073741823, speed 143079421 seeds per second
Found 1, trying 1073741824 - 1107296255, speed 142974943 seeds per second
Found 1, trying 1107296256 - 1140850687, speed 142876936 seeds per second
Found 1, trying 1140850688 - 1174405119, speed 142606336 seeds per second
Found 1, trying 1174405120 - 1207959551, speed 142352135 seeds per second
Found 1, trying 1207959552 - 1241513983, speed 142112888 seeds per second
Found 1, trying 1241513984 - 1275068415, speed 142049654 seeds per second
Found 1, trying 1275068416 - 1308622847, speed 141831859 seeds per second
Found 1, trying 1308622848 - 1342177279, speed 141625849 seeds per second
Found 1, trying 1342177280 - 1375731711, speed 141430693 seeds per second
Found 1, trying 1375731712 - 1409286143, speed 141100688 seeds per second
Found 1, trying 1409286144 - 1442840575, speed 140787826 seeds per second
Found 1, trying 1442840576 - 1476395007, speed 140627736 seeds per second
Found 1, trying 1476395008 - 1509949439, speed 140475262 seeds per second
Found 1, trying 1509949440 - 1543503871, speed 140069521 seeds per second
seed = 1531442241
Found 2, trying 1543503872 - 1577058303, speed 139810133 seeds per second
Found 2, trying 1577058304 - 1610612735, speed 139562681 seeds per second
Found 2, trying 1610612736 - 1644167167, speed 139367828 seeds per second
```

目录爆破

两个以上的递归爆破类型选择Cluster bomb

Attack type: Cluster bomb

GET /\$0\$/\$1\$/ HTTP/1.1