

BUUCTF记录-Basic

原创

繁华若有光 于 2021-11-16 17:41:48 发布 3047 收藏

分类专栏: [BUUCTF](#) 文章标签: [web安全](#) [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/yx1996103/article/details/121360312>

版权



[BUUCTF 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

本机环境: Windows10

目录

一、Linux Labs 1

二、BUU LFI Course 1

三、Upload-Labs-Linux

1、第1关

2、第2关

3、第3关

4、第6关

5、第7关

一、Linux Labs 1

题目提示:

ssh 用户名: root 密码: 123456 地址和端口为动态分配的。

解题思路:

1. 打开cmd控制台, ssh连接靶机, 然后输入密码

```
ssh -p 25836 root@node4.buuoj.cn
```

2. 现在位于用户目录~, cd切换至根目录/, 查看根目录下所有文件, 发现flag.txt, 查看文件内容

```
root@5f742f6c91b8:~# ls -la
.  ..  .bash_history  .bashrc  .cache  .profile  .ssh
root@5f742f6c91b8:~# cd ../
root@5f742f6c91b8:/# ls -la
.  bd_build  boot  .dockerenv  flag.txt  home  lib64  mnt  proc  run  srv  tmp  var
..  bin      dev  etc         get-pip.py  lib   media  opt  root  sbin  sys  usr
root@5f742f6c91b8:/# cat flag.txt
flag {ccca652f-5164-4143-b509-fdc8cda6cef2}
```

CSDN @繁华若有光

二、BUU LFI Course 1

题目提示：

LFI：本地文件包含

解题思路：

本关考察本地文件包含漏洞，通过该漏洞可以实现目录遍历。通过页面显示的代码可以发现，源代码没有对file变量进行任何过滤，因此可以通过修改传给file的参数读取目标文件：

<http://acc14be3-18b9-40d0-8085-4a01808dce83.node4.buuoj.cn:81/?file=/flag>

修改/flag为其他路径，还可以访问靶机的其他内容。

三、Upload-Labs-Linux

1、第1关

使用火狐浏览器渗透测试版，关闭前端JS：



然后就可以上传php文件了

2、第2关

过滤代码为：

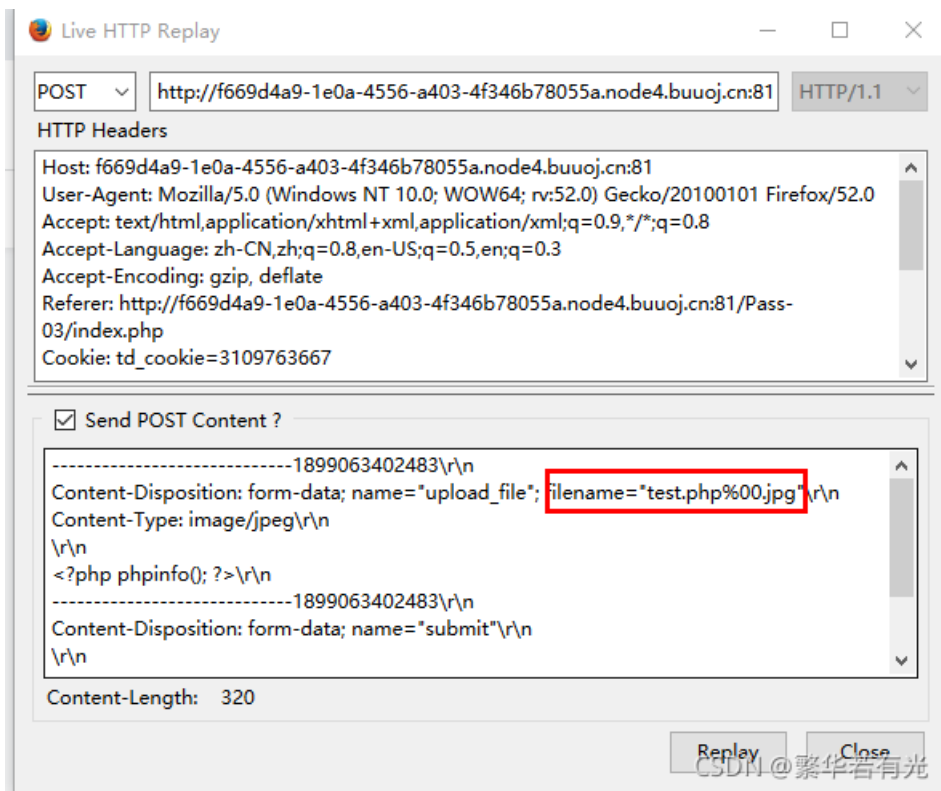
```
if (($FILES['upload_file']['type'] == 'image/jpeg') || ($FILES['upload_file']['type'] == 'image/png') ||
    $temp_file = $FILES['upload_file']['tmp_name'];
```

抓包，将content-type修改为代码中允许的类型。

3、第3关

```
$deny_ext = array('.asp', '.aspx', '.php', '.jsp');
$file_name = trim($FILES['upload_file']['name']);
$file_name = deldot($file_name); //删除文件名末尾的点
$file_ext = strrchr($file_name, '.'); //截取最后一个.后的字符串
$file_ext = strtolower($file_ext); //转换为小写
$file_ext = str_ireplace('::$DATA', '', $file_ext); //去除字符串::$DATA
$file_ext = trim($file_ext); //收尾去空
```

源代码使用了黑名单，且截取文件名最后最后一个.后的字符串作为文件名后缀。可以考虑：1) 修改本机文件后缀，比如php1、php2、phtml、php5等；2) 抓包，修改filename字段，采用%00进行截断：



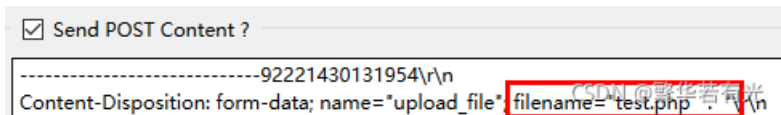
第4、5关的黑名单更加丰富，但是方法2仍然有效！

4、第6关

本关在过滤的步骤中，相比前面，去掉了最后一个首尾去空的步骤

```
$file_ext = trim($file_ext); //首尾去空
```

因此除了前面采用%00进行截断的方法，还可以采用在文件名中添加空格进行绕过的方法：



5、第7关

本关缺少删除文件名末尾的点的步骤：

```
$file_name = deldot($file_name); //删除文件名末尾的点
```



[创作打卡挑战赛](#) >

赢取流量/现金/CSDN周边激励大奖