18 - Attacking Common Applications

基于 Web 的应用程序在我们作为渗透测试人员遇到的大多数（如果不是全部）环境中都很普遍。在我们的评估过程中，我们将遇到各种各样的 Web 应用程序，例如内容管理系统（CMS）、自定义 Web 应用程序、开发人员和系统管理员使用的 Intranet 门户、代码存储库、网络监控工具、票证系统、Wiki、知识库、问题跟踪器、servlet 容器应用程序等。在许多不同的环境中找到相同的应用程序是很常见的。虽然应用程序在一个环境中可能不易受到攻击，但在下一个环境中可能会配置错误或未打补丁。评估员需要牢牢掌握列举和攻击本模块中涵盖的常见应用程序。

Web 应用程序是可以通过 Web 浏览器访问的交互式应用程序。Web 应用程序通常采用客户端-服务器架构来运行和处理交互。它们通常由运行在客户端（浏览器）上的前端组件（网站界面或“用户看到的内容”）和运行在服务器端（后端服务器/数据库）的其他后端组件（Web 应用程序源代码）组成。有关 Web 应用程序结构和功能的深入研究，请查看 Web 应用程序简介🔗模块。

所有类型的 Web 应用程序（商业、开源和自定义）都可能遭受相同类型的漏洞和错误配置，即 OWASP 前 10 大🔗中涵盖的前 10 大 Web 应用程序风险。虽然我们可能会遇到许多常见应用程序的易受攻击版本，这些应用程序存在已知的（公共）漏洞，例如 SQL 注入、XSS、远程代码执行错误、本地文件读取和不受限制的文件上传，但了解我们如何滥用其中许多应用程序的内置功能来实现远程代码执行对我们来说同样重要。

应用程序发现和枚举

为了有效地管理其网络，组织应维护（并持续更新）资产清单，其中包括所有网络连接的设备（服务器、工作站、网络设备等）、已安装的软件和整个环境中正在使用的应用程序。如果组织不确定其网络上存在什么，它将如何知道要保护什么以及存在哪些潜在的漏洞？组织应该知道应用程序是在本地安装还是由第三方托管，它们当前的补丁级别，它们是否处于或接近生命周期结束，能够检测到网络中的任何流氓应用程序（或“影子 IT”），并对每个应用程序有足够的可见性，以确保它们得到强（非默认）密码的充分保护， 理想情况下，启用 Multi-Factor Authentication。某些应用程序具有管理门户，这些门户可以限制为只能从特定 IP 地址或主机本身 （localhost） 访问。

现实情况是，许多组织并不了解其网络上的所有内容，而一些组织的可见性非常低，我们可以帮助他们解决这个问题。我们执行的普查对我们的客户非常有益，可以帮助他们增强或开始构建资产清单。我们很可能会识别出被遗忘的应用程序、试用许可证可能已过期并转换为不需要身份验证的版本的软件演示版本（在 Splunk 的情况下）、具有默认/弱凭据的应用程序、未经授权/配置错误的应用程序以及存在公共漏洞的应用程序。我们可以将此数据作为报告中结果的组合提供给我们的客户（即，具有默认凭证 `admin：admin` 的应用程序，作为附录，例如映射到主机的已识别服务列表或补充扫描数据）。我们甚至可以更进一步，让我们的客户了解我们每天使用的一

些工具，这样他们就可以开始对他们的网络进行定期和主动的侦察，并在渗透测试人员或更糟糕的攻击者首先发现它们之前找到漏洞。

Nmap - Web Discovery

```
Chenduoduo@htb[/htb]$ nmap -p 80,443,8000,8080,8180,8888,10000 --open -oA web_discovery -iL scope_list
```

```
Chenduoduo@htb[/htb]$ cat scope_list

app.inlanefreight.local
dev.inlanefreight.local
drupal-dev.inlanefreight.local
drupal-qa.inlanefreight.local
drupal-acc.inlanefreight.local
drupal.inlanefreight.local
blog-dev.inlanefreight.local
blog.inlanefreight.local
app-dev.inlanefreight.local
jenkins-dev.inlanefreight.local
jenkins.inlanefreight.local
web01.inlanefreight.local
gitlab-dev.inlanefreight.local
gitlab.inlanefreight.local
support-dev.inlanefreight.local
support.inlanefreight.local
inlanefreight.local
10.129.201.50
```

我们可以从常见 Web 端口的 Nmap 扫描开始。我通常会使用端口 `80,443,8000,8080,8180,8888,10000` 进行初始扫描，然后针对此初始扫描运行 EyeWitness 或 Aquatone（或同时运行两者，具体取决于第一次的结果）。在查看最常见端口的屏幕截图报告时，我可能会对前 10,000 个端口或所有 TCP 端口运行更彻底的 Nmap 扫描，具体取决于范围的大小。由于枚举是一个迭代过程，我们将针对我们执行的任何后续 Nmap 扫描运行 Web 屏幕截图工具，以确保最大覆盖率。

```
Chenduoduo@htb[/htb]$ sudo  nmap -p 80,443,8000,8080,8180,8888,10000 --open -oA web_discovery -iL scope_list

Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-07 21:49 EDT
Stats: 0:00:07 elapsed; 1 hosts completed (4 up), 4 undergoing SYN Stealth Scan
```

```
SYN Stealth Scan Timing: About 81.24% done; ETC: 21:49 (0:00:01 remaining)

Nmap scan report for app.inlanefreight.local (10.129.42.195)
Host is up (0.12s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap scan report for app-dev.inlanefreight.local (10.129.201.58)
Host is up (0.12s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8000/tcp open  http-alt
8009/tcp open  ajp13
8080/tcp open  http-proxy
8180/tcp open  unknown
8888/tcp open  sun-answerbook

Nmap scan report for gitlab-dev.inlanefreight.local (10.129.201.88)
Host is up (0.12s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8081/tcp open  blackice-icecap

Nmap scan report for 10.129.201.50
Host is up (0.13s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
8000/tcp open  http-alt
8080/tcp open  http-proxy
8089/tcp open  unknown

<SNIP>
```

```
Chenduoduo@htb[/htb]$ sudo nmap --open -sV 10.129.42.94

Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-07 21:58 EDT
Nmap scan report for 10.129.201.50
Host is up (0.13s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8000/tcp open  http          Splunkd httpd
8080/tcp open  http          Indy httpd 17.3.33.2830 (Paessler PRTG
bandwidth monitor)
8089/tcp open  ssl/http      Splunkd httpd (free license; remote login
disabled)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 38.63 seconds
```

EyeWitness

首先是 EyeWitness。如前所述，EyeWitness 可以从 Nmap 和 Nessus 获取 XML 输出，并使用 Selenium 创建包含各个端口上每个 Web 应用程序的屏幕截图的报告。它还将更进一步，尽可能对应用程序进行分类，对它们进行指纹识别，并根据应用程序建议默认凭据。还可以为其提供 IP 地址和 URL 列表，并告知将 `http://` 和 `https://` 放在每个地址的前面。它将对 IP 执行 DNS 解析，并且可以为一组特定的端口提供尝试连接和屏幕截图。

```
Chenduoduo@htb[/htb]$ sudo apt install eyewitness
```

```
Chenduoduo@htb[/htb]$ eyewitness -h

usage: EyeWitness.py [--web] [-f Filename] [-x Filename.xml]
                     [--single Single URL] [--no-dns] [--timeout
Timeout]
                     [--jitter # of Seconds] [--delay # of Seconds]
                     [--threads # of Threads]
                     [--max-retries Max retries on a timeout]
                     [-d Directory Name] [--results Hosts Per Page]
                     [--no-prompt] [--user-agent User Agent]
                     [--difference Difference Threshold]
                     [--proxy-ip 127.0.0.1] [--proxy-port 8080]
                     [--proxy-type socks5] [--show-selenium] [--resolve]
                     [--add-http-ports ADD_HTTP_PORTS]
                     [--add-https-ports ADD_HTTPS_PORTS]
                     [--only-ports ONLY_PORTS] [--prepend-https]
                     [--selenium-log-path SELENIUM_LOG_PATH] [--resume
ew.db]
                     [--ocr]

EyeWitness is a tool used to capture screenshots from a list of URLs

Protocols:
  --web                 HTTP Screenshot using Selenium

Input Options:
  -f Filename           Line-separated file containing URLs to capture
  -x Filename.xml       Nmap XML or .Nessus file
  --single Single URL   Single URL/Host to capture
  --no-dns              Skip DNS resolution when connecting to websites

Timing Options:
  --timeout Timeout     Maximum number of seconds to wait while
requesting a
                        web page (Default: 7)
  --jitter # of Seconds
                        Randomize URLs and add a random delay between
requests
  --delay # of Seconds  Delay between the opening of the navigator and
taking
                        the screenshot
  --threads # of Threads
                        Number of threads to use while using file based
input
  --max-retries Max retries on a timeout
                        Max retries on timeouts

<SNIP>
```

运行默认的 `--web` 选项，使用发现扫描的 Nmap XML 输出作为输入来截取屏幕截图。

```
Chenduoduo@htb[/htb]$ eyewitness --web -x web_discovery.xml -d
inlanefreight_eyewitness

################################################################################
########
#                                  EyeWitness
#
################################################################################
########
#           FortyNorth Security - https://www.fortynorthsecurity.com
#
################################################################################
########

Starting Web Requests (26 Hosts)
Attempting to screenshot http://app.inlanefreight.local
Attempting to screenshot http://app-dev.inlanefreight.local
Attempting to screenshot http://app-dev.inlanefreight.local:8000
Attempting to screenshot http://app-dev.inlanefreight.local:8080
Attempting to screenshot http://gitlab-dev.inlanefreight.local
Attempting to screenshot http://10.129.201.50
Attempting to screenshot http://10.129.201.50:8000
Attempting to screenshot http://10.129.201.50:8080
Attempting to screenshot http://dev.inlanefreight.local
Attempting to screenshot http://jenkins-dev.inlanefreight.local
Attempting to screenshot http://jenkins-dev.inlanefreight.local:8000
Attempting to screenshot http://jenkins-dev.inlanefreight.local:8080
Attempting to screenshot http://support-dev.inlanefreight.local
Attempting to screenshot http://drupal-dev.inlanefreight.local
[*] Hit timeout limit when connecting to http://10.129.201.50:8000,
retrying
Attempting to screenshot http://jenkins.inlanefreight.local
Attempting to screenshot http://jenkins.inlanefreight.local:8000
Attempting to screenshot http://jenkins.inlanefreight.local:8080
Attempting to screenshot http://support.inlanefreight.local
[*] Completed 15 out of 26 services
Attempting to screenshot http://drupal-qa.inlanefreight.local
Attempting to screenshot http://web01.inlanefreight.local
Attempting to screenshot http://web01.inlanefreight.local:8000
Attempting to screenshot http://web01.inlanefreight.local:8080
Attempting to screenshot http://inlanefreight.local
Attempting to screenshot http://drupal-acc.inlanefreight.local
Attempting to screenshot http://drupal.inlanefreight.local
Attempting to screenshot http://blog-dev.inlanefreight.local
```

```
Finished in 57.859838008880615 seconds

[*] Done! Report written in the
/home/mrb3n/Projects/inlanfreight/inlanefreight_eyewitness folder!
Would you like to open the report now? [Y/n]
```

Using Aquatone

Aquatone 类似于 EyeWitness，当提供主机的 `.txt` 文件或带有 `-nmap` 标志的 Nmap `.xml` 文件时，可以截取屏幕截图。我们可以自己编译 Aquatone 或下载预编译的二进制文件。下载二进制文件后，我们只需要提取它，就可以开始了。

```
Chenduoduo@htb[/htb]$ wget
https://github.com/michenriksen/aquatone/releases/download/v1.7.0/aquato
ne_linux_amd64_1.7.0.zip
```

```
Chenduoduo@htb[/htb]$ unzip aquatone_linux_amd64_1.7.0.zip

Archive:  aquatone_linux_amd64_1.7.0.zip
  inflating: aquatone
  inflating: README.md
  inflating: LICENSE.txt
```

我们可以将其移动到 `$PATH` 中的某个位置，例如 `/usr/local/bin`，以便能够从任何地方调用该工具，或者将二进制文件放在我们的工作（比如 scans）目录中。这是个人喜好，但通常最有效的方法是使用大多数可用工具构建我们的攻击 VM，而无需不断更改目录或从其他目录调用它们。

```
Chenduoduo@htb[/htb]$ echo $PATH

/home/mrb3n/.local/bin:/snap/bin:/usr/sandbox/:/usr/local/bin:/usr/bin:/
bin:/usr/local/games:/usr/games:/usr/share/games:/usr/local/sbin:/usr/sb
in:/sbin:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
```

在这个例子中，我们为工具提供了与 Nmap 相同的 `web_discovery.xml` 输出，指定了 `-nmap` 标志，然后我们开始了比赛。

```
Chenduoduo@htb[/htb]$ cat web_discovery.xml | ./aquatone -nmap

aquatone v1.7.0 started at 2021-09-07T22:31:03-04:00
```

```
Targets    : 65
Threads    : 6
Ports      : 80, 443, 8000, 8080, 8443
Output dir : .

http://web01.inlanefreight.local:8000/: 403 Forbidden
http://app.inlanefreight.local/: 200 OK
http://jenkins.inlanefreight.local/: 403 Forbidden
http://app-dev.inlanefreight.local/: 200
http://app-dev.inlanefreight.local/: 200
http://app-dev.inlanefreight.local:8000/: 403 Forbidden
http://jenkins.inlanefreight.local:8000/: 403 Forbidden
http://web01.inlanefreight.local:8080/: 200
http://app-dev.inlanefreight.local:8000/: 403 Forbidden
http://10.129.201.50:8000/: 200 OK

<SNIP>

http://web01.inlanefreight.local:8000/: screenshot successful
http://app.inlanefreight.local/: screenshot successful
http://app-dev.inlanefreight.local/: screenshot successful
http://jenkins.inlanefreight.local/: screenshot successful
http://app-dev.inlanefreight.local/: screenshot successful
http://app-dev.inlanefreight.local:8000/: screenshot successful
http://jenkins.inlanefreight.local:8000/: screenshot successful
http://app-dev.inlanefreight.local:8000/: screenshot successful
http://app-dev.inlanefreight.local:8080/: screenshot successful
http://app.inlanefreight.local/: screenshot successful

<SNIP>

Calculating page structures... done
Clustering similar pages... done
Generating HTML report... done

Writing session file...Time:
 - Started at  : 2021-09-07T22:31:03-04:00
 - Finished at : 2021-09-07T22:31:36-04:00
 - Duration    : 33s

Requests:
 - Successful : 65
 - Failed     : 0

 - 2xx : 47
```

```
  - 3xx : 0
  - 4xx : 18
  - 5xx : 0

Screenshots:
  - Successful : 65
  - Failed     : 0

Wrote HTML report to: aquatone_report.html
```

即使有上述 26 个主机，此报告也将节省我们的时间。现在想象一下一个有 500 或 5,000 个主机的环境！打开报告后，我们看到报告被分为几类， `高价值目标 （High Value Targets`） 排在第一位，通常是最 “多汁” 的主机。我在非常大的环境中运行 EyeWitness 并生成了包含数百页的报告，需要花费数小时才能完成。通常，非常大的报告会深埋其中有趣的主机，因此值得回顾整个事情并戳戳/研究我们不熟悉的任何应用程序。在外部渗透测试期间，我发现介绍部分中提到的 `ManageEngine OpManager` 应用程序深深地隐藏在一个非常大的报告中。此实例配置了默认凭证 `admin：admin`，并对 Internet 完全开放。我能够通过运行 PowerShell 脚本登录并实现代码执行。OpManager 应用程序在 Domain Admin 帐户的上下文中运行，这导致内部网络完全受损。

在下面的报告中，我会立即很高兴看到 Tomcat 出现在任何评估中（尤其是在外部渗透测试期间），并将在 `/manager` 和 `/host-manager` 端点上尝试默认凭据。如果我们可以访问其中任何一个，我们就可以上传恶意的 WAR 文件，并使用 JSP 代码在底层主机上实现远程代码执

行。本模块稍后将对此进行详细介绍。

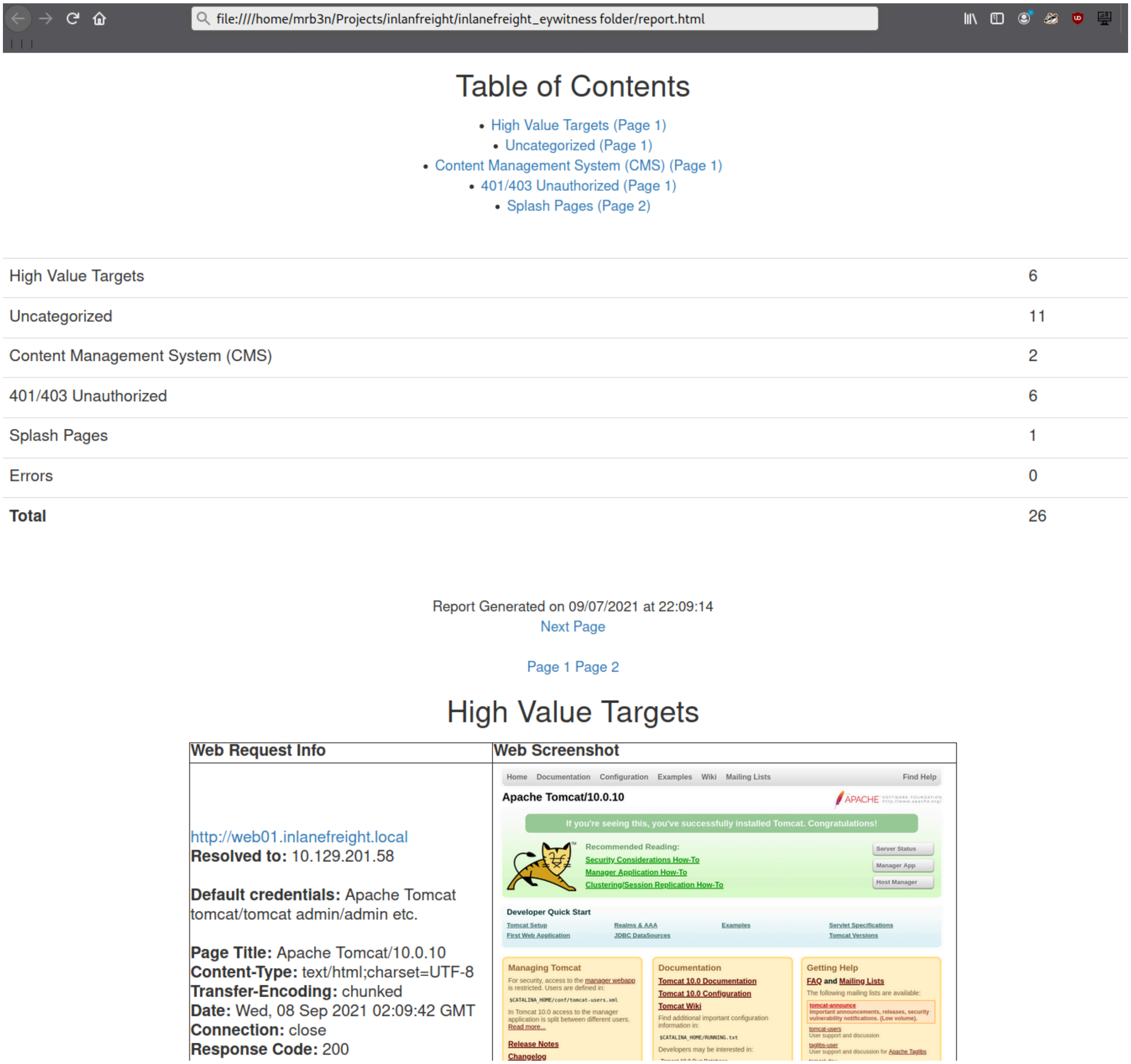
file:///home/mrb3n/Projects/inlanefreight/inlanefreight_eywitness folder/report.html

Table of Contents

- High Value Targets (Page 1)
- Uncategorized (Page 1)
- Content Management System (CMS) (Page 1)
- 401/403 Unauthorized (Page 1)
- Splash Pages (Page 2)

High Value Targets	6
Uncategorized	11
Content Management System (CMS)	2
401/403 Unauthorized	6
Splash Pages	1
Errors	0
Total	26

Report Generated on 09/07/2021 at 22:09:14

Next Page

Page 1 Page 2

High Value Targets

Web Request Info	Web Screenshot
http://web01.inlanefreight.local **Resolved to:** 10.129.201.58 **Default credentials:** Apache Tomcat tomcat/tomcat admin/admin etc. **Page Title:** Apache Tomcat/10.0.10 **Content-Type:** text/html;charset=UTF-8 **Transfer-Encoding:** chunked **Date:** Wed, 08 Sep 2021 02:09:42 GMT **Connection:** close **Response Code:** 200	

继续浏览报告，看起来下一个是 `http://inlanefreight.local` 主网站。自定义 Web 应用程序总是值得测试的，因为它们可能包含各种各样的漏洞。在这里，我还有兴趣查看该网站是否正在运行流行的 CMS，例如 WordPress、Joomla 或 Drupal。下一个应用程序 `http://support-dev.inlanefreight.local` 很有趣，因为它似乎正在运行 osTicket，多年来，它一直受到各种严重漏洞的困扰。支持工单系统特别有趣，因为我们可能能够登录并访问敏感信息。如果社会工程在范围内，我们可能能够与客户支持人员互动，甚至纵系统为公司的域注册一个有效的电子邮件地址，我们可以利用该地址来访问其他服务。

最后一件在 IppSec 的 HTB 每周发布框 Delivery 中进行了演示。这个特定的框值得研究，因为它通过探索某些常见应用程序的内置功能展示了什么是可能的。我们将在本模块后面更深入地介绍 osTicket。

```
10.129.90.48 app.inlanefreight.local
10.129.90.48 dev.inlanefreight.local
10.129.90.48 drupal-dev.inlanefreight.local
10.129.90.48 drupal-qa.inlanefreight.local
10.129.90.48 drupal-acc.inlanefreight.local
10.129.90.48 drupal.inlanefreight.local
10.129.90.48 blog.inlanefreight.local
```

内容管理系统（CMS）

Content Management Systems