Content Discovery

Learn the various ways of discovering hidden or private content on a webserver that could lead to new vulnerabilities.

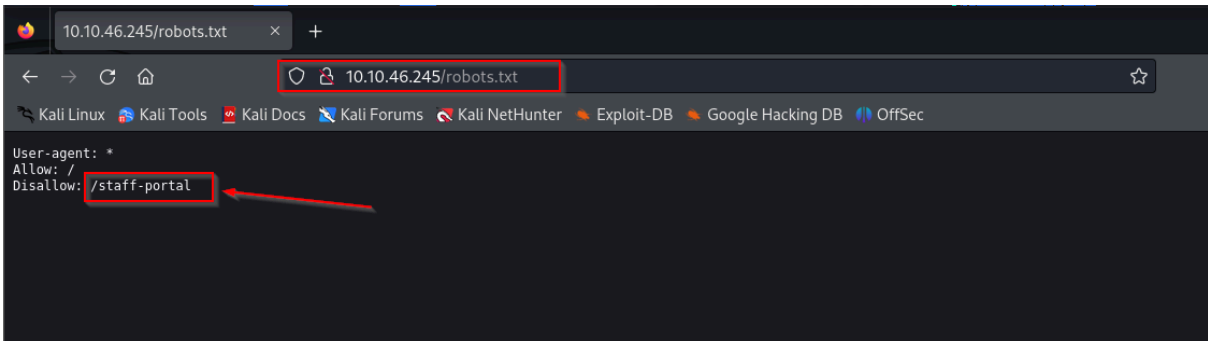
Question	**Answer**
What is the Content Discovery method that begins with M?	Manually
What is the Content Discovery method that begins with A?	Automated
What is the Content Discovery method that begins with O?	OSINT

Task 2 Manual Discovery - Robots.txt

What is the directory in the robots.txt that isn't allowed to be viewed by web crawlers?

Answer: /staff-portal

- ➔ I visited the robot.txt page



```
User-agent: *
Allow: /
Disallow: /staff-portal
```

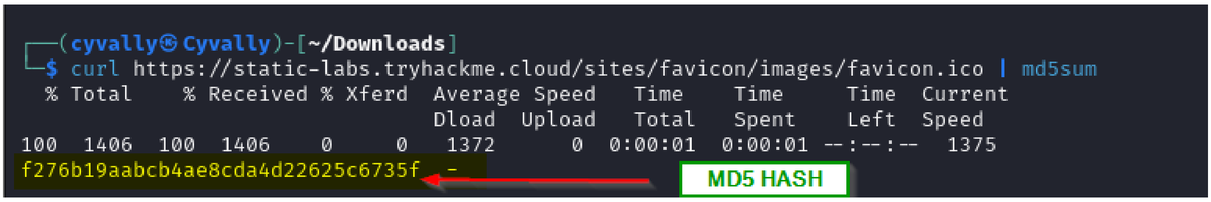
Task 3 Manual Discovery - Favicon

What framework did the favicon belong to?

Answer: cgiirc

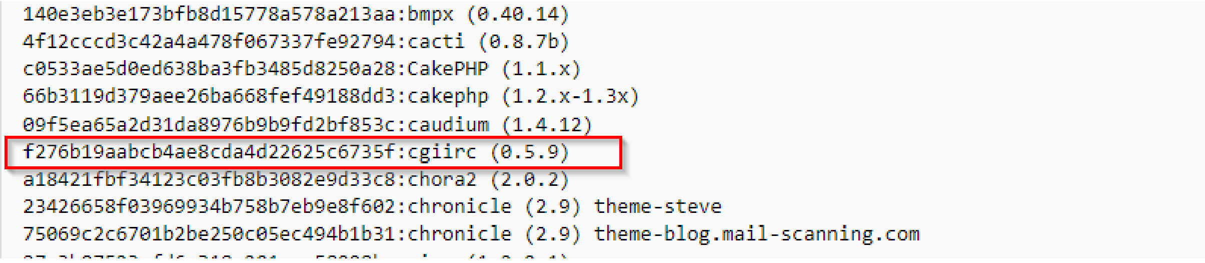
- ➔ I downloaded the favicon and gt its md5 hash value

Command: curl https://static-labs.tryhackme.cloud/sites/favicon/images/favicon.ico | md5sum



```
┌──(cyvally㉿Cyvally)-[~/Downloads]
└─$ curl https://static-labs.tryhackme.cloud/sites/favicon/images/favicon.ico | md5sum
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1406  100  1406    0     0   1372      0  0:00:01  0:00:01 --:--:--  1375
f276b19aabcb4ae8cda4d22625c6735f  -
```

- ➔ then lookup on the https://wiki.owasp.org/index.php/OWASP_favicon_database.



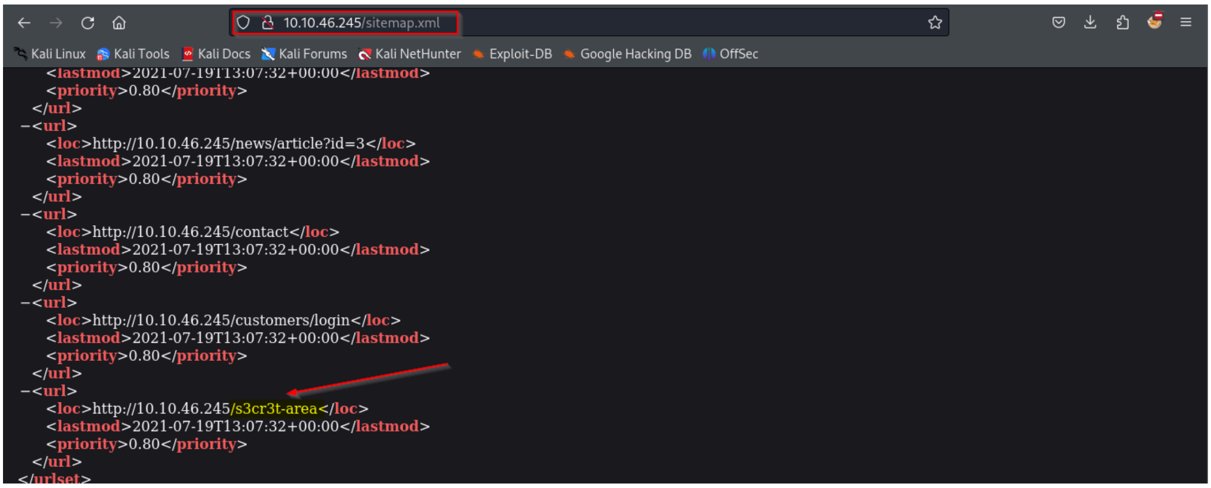
```
140e3eb3e173bfb8d15778a578a213aa:bmpx (0.40.14)
4f12cccd3c42a4a478f067337fe92794:cacti (0.8.7b)
c0533ae5d0ed638ba3fb3485d8250a28:CakePHP (1.1.x)
66b3119d379aee26ba668fef49188dd3:cakephp (1.2.x-1.3x)
09f5ea65a2d31da8976b9b9fd2bf853c:caudium (1.4.12)
f276b19aabcb4ae8cda4d22625c6735f:cgiirc (0.5.9)
a18421fbf34123c03fb8b3082e9d33c8:chora2 (2.0.2)
23426658f03969934b758b7eb9e8f602:chronicle (2.9) theme-steve
75069c2c6701b2be250c05ec494b1b31:chronicle (2.9) theme-blog.mail-scanning.com
```

Task 4 Manual Discovery - Sitemap.xml

What is the path of the secret area that can be found in the sitemap.xml file?

Answer: /s3cr3t-area

- ➔ I visited the Sitemap.xml page



```
    <lastmod>2021-07-19T13:07:32+00:00</lastmod>
    <priority>0.80</priority>
  </url>
-<url>
    <loc>http://10.10.46.245/news/article?id=3</loc>
    <lastmod>2021-07-19T13:07:32+00:00</lastmod>
    <priority>0.80</priority>
  </url>
-<url>
    <loc>http://10.10.46.245/contact</loc>
    <lastmod>2021-07-19T13:07:32+00:00</lastmod>
    <priority>0.80</priority>
  </url>
-<url>
    <loc>http://10.10.46.245/customers/login</loc>
    <lastmod>2021-07-19T13:07:32+00:00</lastmod>
    <priority>0.80</priority>
  </url>
-<url>
    <loc>http://10.10.46.245/s3cr3t-area</loc>
    <lastmod>2021-07-19T13:07:32+00:00</lastmod>
    <priority>0.80</priority>
  </url>
</urlset>
```

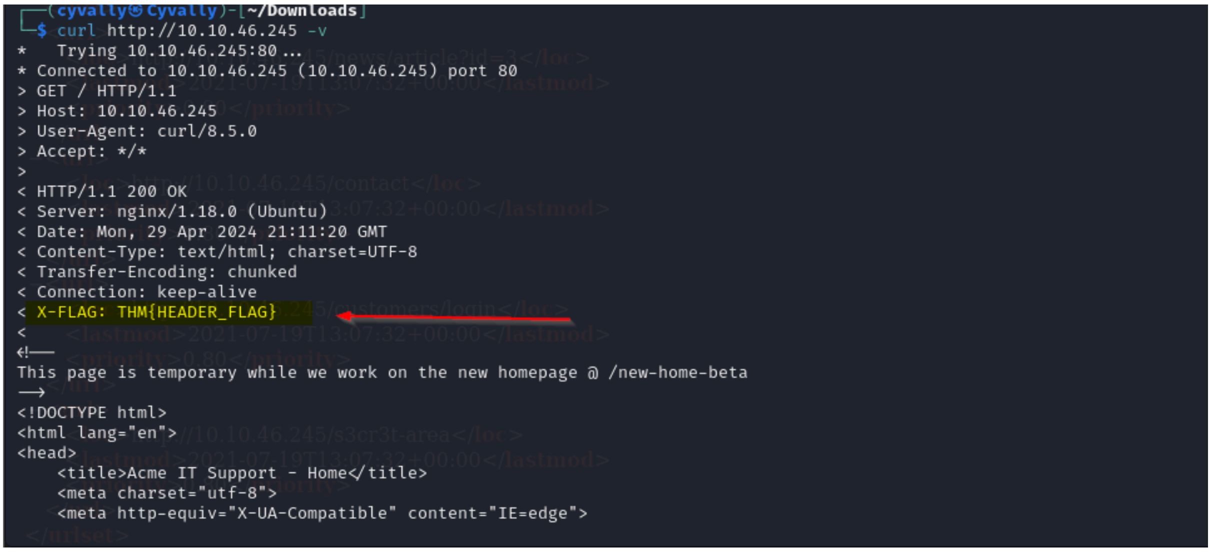
Task 5 Manual Discovery - HTTP Headers

What is the flag value from the X-FLAG header?

Answer: THM{HEADER_FLAG}

- ➔ I outputted the headers in the target web app

Command: curl http://10.10.46.245 -v



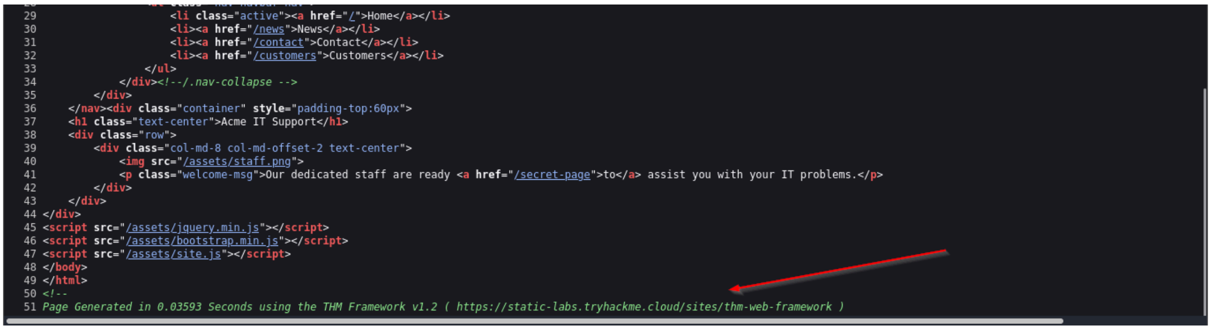
```
┌──(cyvally㉿cyvally)-[~/Downloads]
└─$ curl http://10.10.46.245 -v
*   Trying 10.10.46.245:80 ...
* Connected to 10.10.46.245 (10.10.46.245) port 80
> GET / HTTP/1.1
> Host: 10.10.46.245
> User-Agent: curl/8.5.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: nginx/1.18.0 (Ubuntu)
< Date: Mon, 29 Apr 2024 21:11:20 GMT
< Content-Type: text/html; charset=UTF-8
< Transfer-Encoding: chunked
< Connection: keep-alive
< X-FLAG: THM{HEADER_FLAG}
<
<!—
This page is temporary while we work on the new homepage @ /new-home-beta
—>
<!DOCTYPE html>
<html lang="en">
<head>
    <title>Acme IT Support - Home</title>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
```

Task 6 Manual Discovery - Framework Stack

What is the flag from the framework's administration portal?

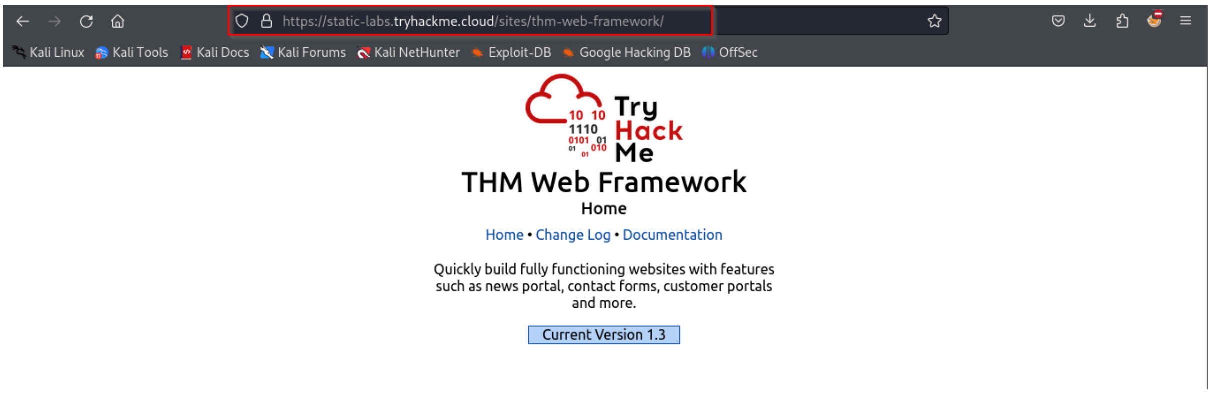
Answer: THM{CHANGE_DEFAULT_CREDENTIALS}

- ➔ I Looked at the page source of the Acme IT Support website (http://10.10.46.245), I see a comment at the end of every page



```
                    <li class="active"><a href="/">Home</a></li>
                    <li><a href="/news">News</a></li>
                    <li><a href="/contact">Contact</a></li>
                    <li><a href="/customers">Customers</a></li>
                </ul>
            </div><!--/.nav-collapse -->
        </div>
    </nav><div class="container" style="padding-top:60px">
    <h1 class="text-center">Acme IT Support</h1>
    <div class="row">
        <div class="col-md-8 col-md-offset-2 text-center">
            <img src="/assets/staff.png">
            <p class="welcome-msg">Our dedicated staff are ready <a href="/secret-page">to</a> assist you with your IT problems.</p>
        </div>
    </div>
</div>
<script src="/assets/jquery.min.js"></script>
<script src="/assets/bootstrap.min.js"></script>
<script src="/assets/site.js"></script>
</body>
</html>
<!--
Page Generated in 0.03593 Seconds using the THM Framework v1.2 ( https://static-labs.tryhackme.cloud/sites/thm-web-framework )
```

- ➔ I visited the website



https://static-labs.tryhackme.cloud/sites/thm-web-framework/

THM Web Framework

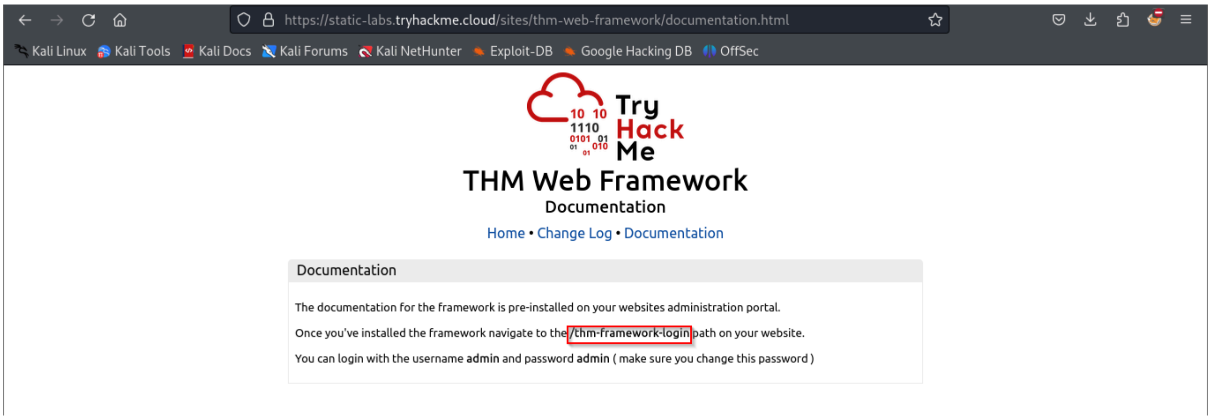
Home

Home • Change Log • Documentation

Quickly build fully functioning websites with features such as news portal, contact forms, customer portals and more.

Current Version 1.3

- ➔ I checked the documentation page and got the path of the framework's administration portal



https://static-labs.tryhackme.cloud/sites/thm-web-framework/documentation.html

THM Web Framework

Documentation

Home • Change Log • Documentation

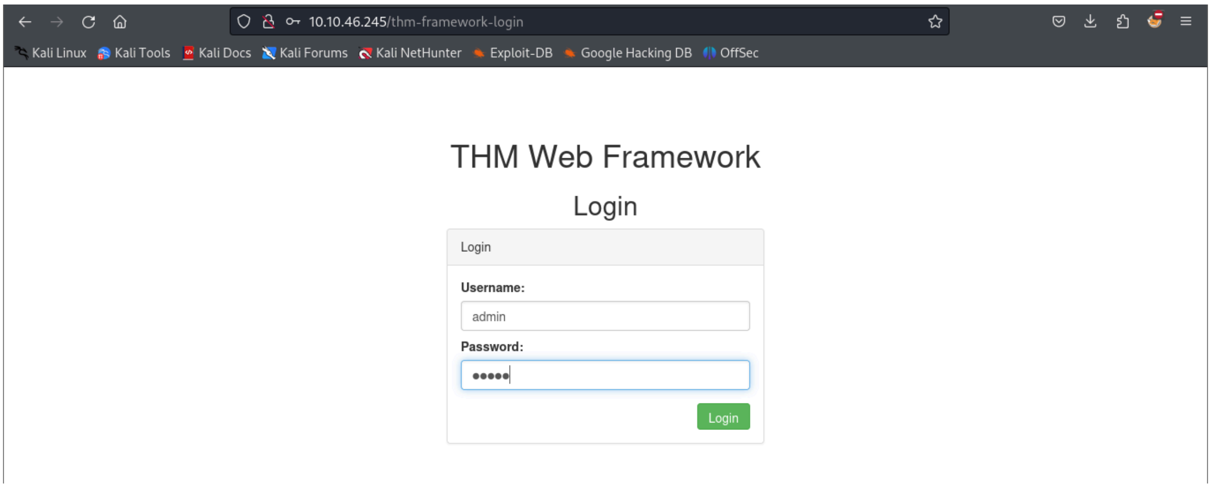
Documentation

The documentation for the framework is pre-installed on your websites administration portal.

Once you've installed the framework navigate to the /thm-framework-login path on your website.

You can login with the username **admin** and password **admin** (make sure you change this password)

- ➔ I login with the username admin and password admin



10.10.46.245/thm-framework-login

THM Web Framework

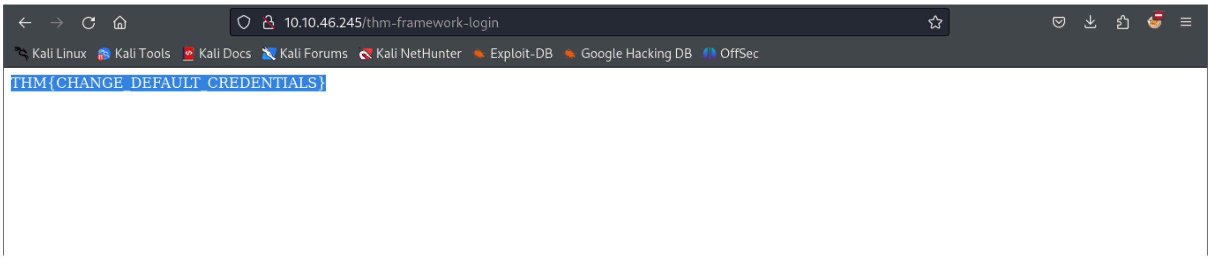
Login

Login

Username: admin

Password: •••••

- ➔ And i got the flag



THM{CHANGE_DEFAULT_CREDENTIALS}

Task 7 OSINT - Google Hacking / Dorking

Question	Answer
What Google dork operator can be used to only show results from a particular site?	site:

Task 8 OSINT - Wappalyzer

Question	Answer
What online tool can be used to identify what technologies a website is running?	Wappalyzer

Task 9 OSINT - Wayback Machine

Question	Answer
What is the website address for the Wayback Machine?	https://archive.org/web/

Task 10 OSINT - GitHub

Question	Answer
What is Git?	version control system

Task 11 OSINT - S3 Buckets

Question	Answer
What URL format do Amazon S3 buckets end in?	.s3.amazonaws.com

Task 12 Automated Discovery

➔ Note: if you are using your kali machine, ensure you have the specified wordlist already, if you do not, then download or clone

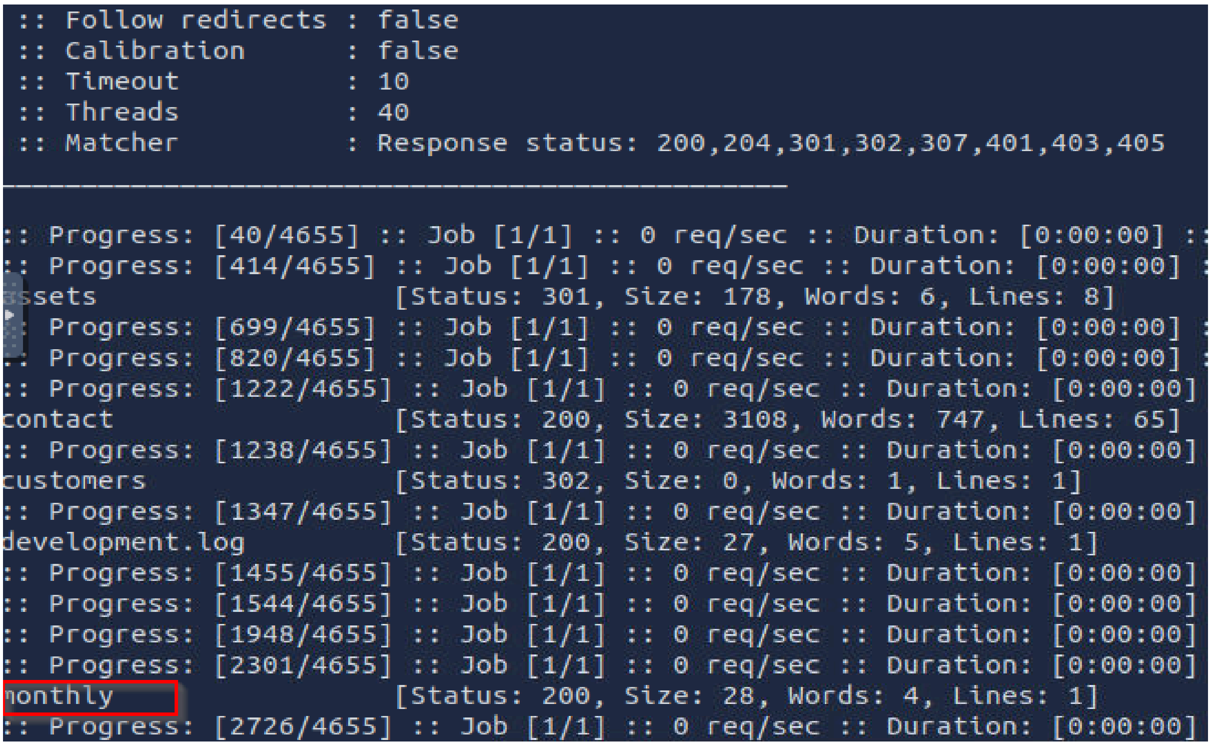
Command: **git clone https://github.com/danielmiessler/SecLists.git**

What is the name of the directory beginning "/mo...." that was discovered?

Answer: **/monthly**

➔ I did directory enumeration

Command: **ffuf -w /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt -u http://10.10.46.245/FUZZ**

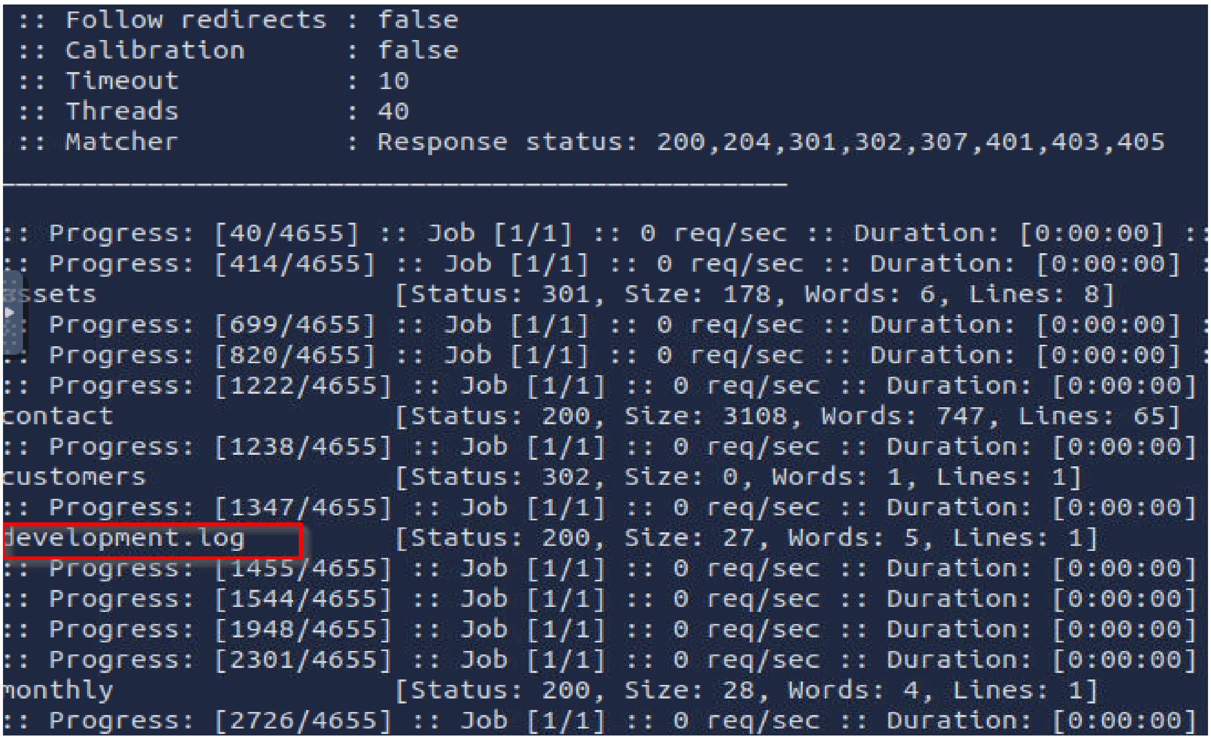


```
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

:: Progress: [40/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] ::
:: Progress: [414/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :
ssets                   [Status: 301, Size: 178, Words: 6, Lines: 8]
   Progress: [699/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :
   Progress: [820/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :
:: Progress: [1222/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
contact                 [Status: 200, Size: 3108, Words: 747, Lines: 65]
:: Progress: [1238/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
customers               [Status: 302, Size: 0, Words: 1, Lines: 1]
:: Progress: [1347/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
development.log         [Status: 200, Size: 27, Words: 5, Lines: 1]
:: Progress: [1455/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
:: Progress: [1544/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
:: Progress: [1948/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
:: Progress: [2301/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
onthly                  [Status: 200, Size: 28, Words: 4, Lines: 1]
:: Progress: [2726/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
```

What is the name of the log file that was discovered?

Answer: /development.log



```
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

:: Progress: [40/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] ::
:: Progress: [414/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :
ssets                   [Status: 301, Size: 178, Words: 6, Lines: 8]
   Progress: [699/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :
   Progress: [820/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :
:: Progress: [1222/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
contact                 [Status: 200, Size: 3108, Words: 747, Lines: 65]
:: Progress: [1238/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
customers               [Status: 302, Size: 0, Words: 1, Lines: 1]
:: Progress: [1347/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
development.log         [Status: 200, Size: 27, Words: 5, Lines: 1]
:: Progress: [1455/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
:: Progress: [1544/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
:: Progress: [1948/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
:: Progress: [2301/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
onthly                  [Status: 200, Size: 28, Words: 4, Lines: 1]
:: Progress: [2726/4655] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00]
```

End!!