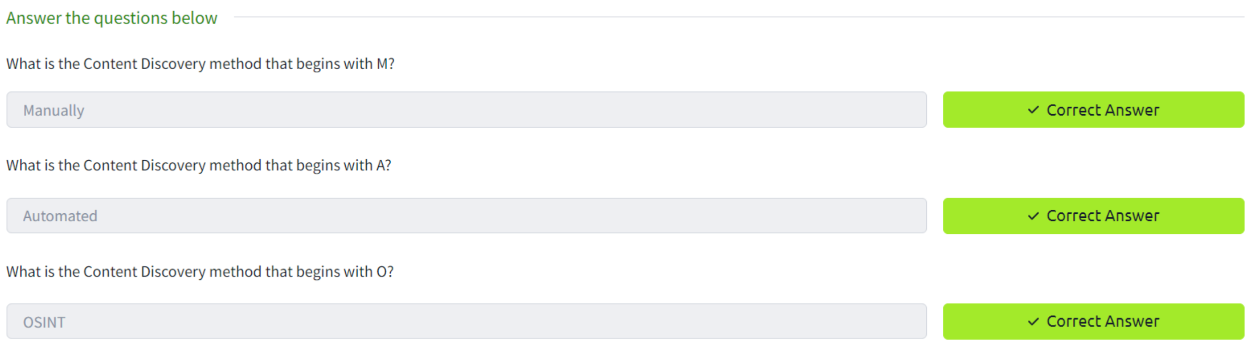
Introduction to Cyber Security

Content Discovery

Task 1:



Answer the questions below

What is the Content Discovery method that begins with M?

Manually

✓ Correct Answer

What is the Content Discovery method that begins with A?

Automated

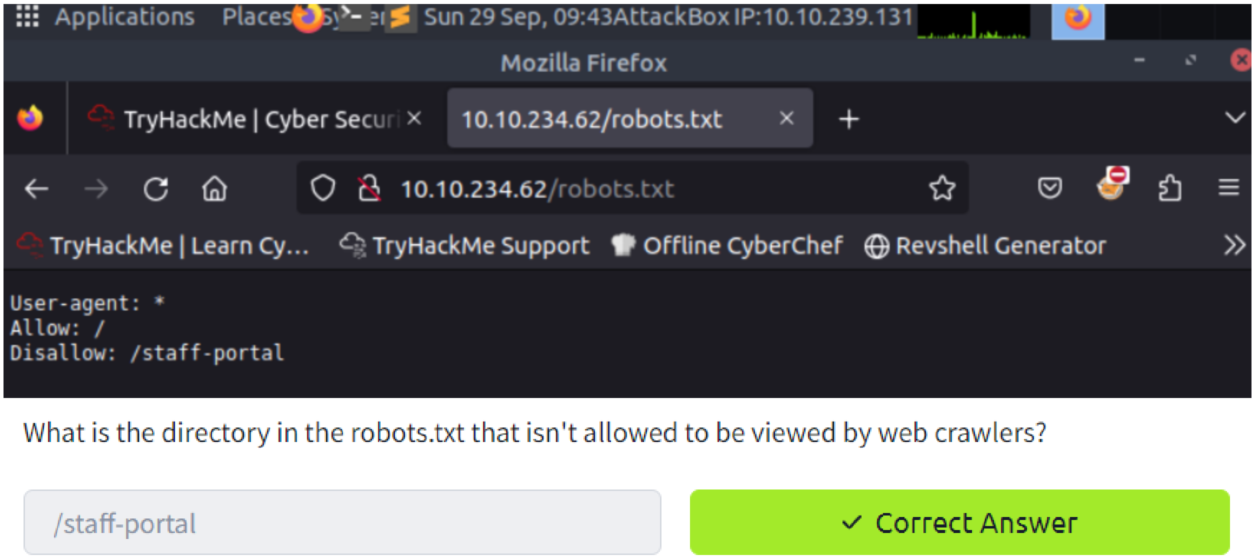
✓ Correct Answer

What is the Content Discovery method that begins with O?

OSINT

✓ Correct Answer

Task 2:



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

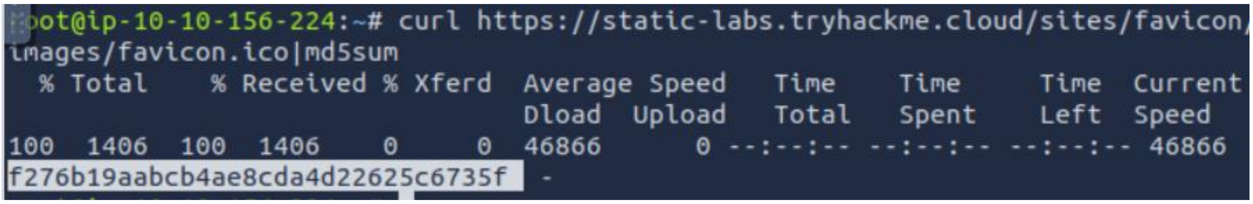
What is the directory in the robots.txt that isn't allowed to be viewed by web crawlers?

/staff-portal

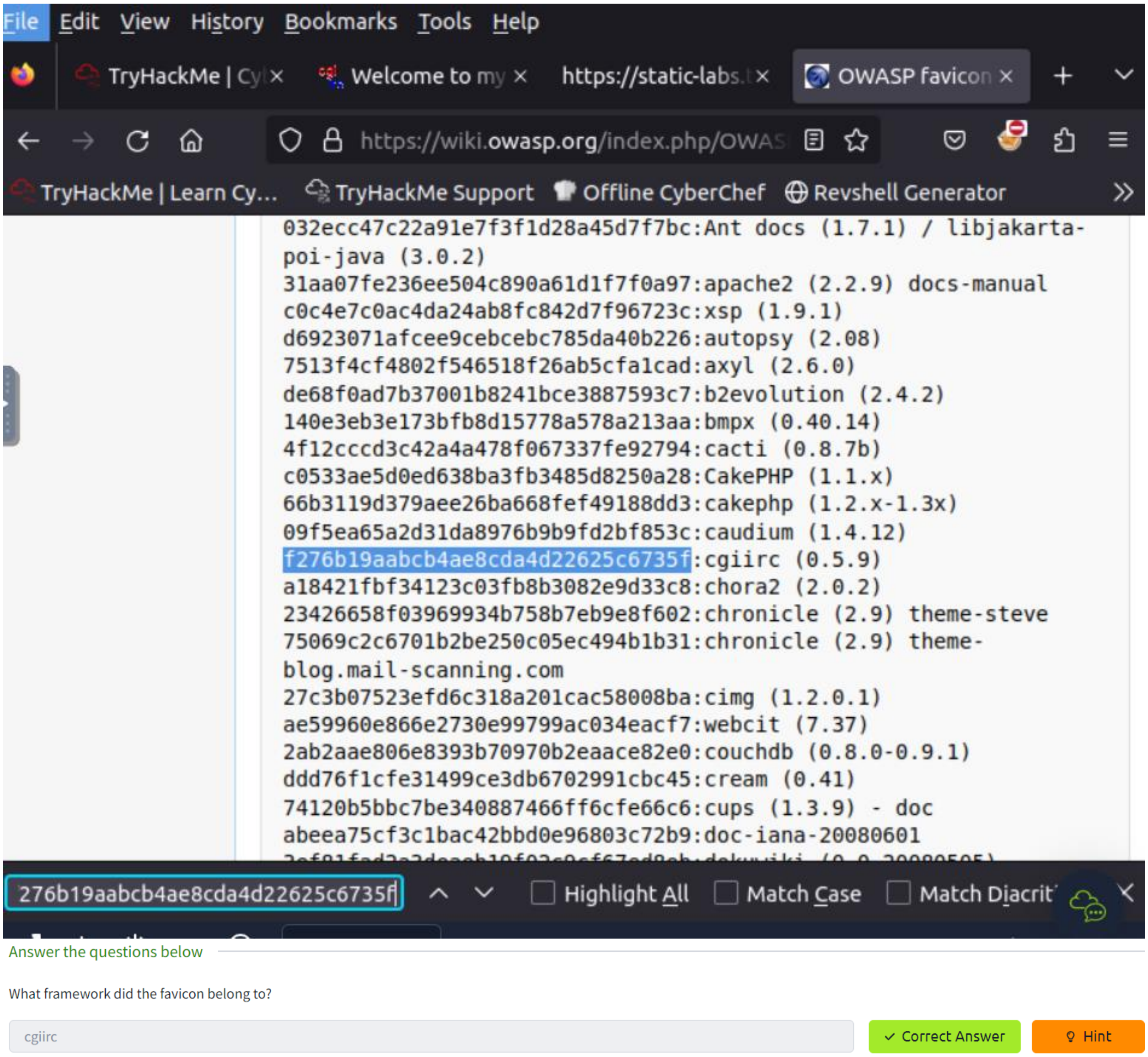
✓ Correct Answer

Task 3:

First goto this URL: https://wiki.owasp.org/index.php/OWASP_favicon_database.



```
oot@ip-10-10-156-224:~# 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  46866      0 --:--:-- --:--:-- --:--:-- 46866
f276b19aabcb4ae8cda4d22625c6735f  -
```



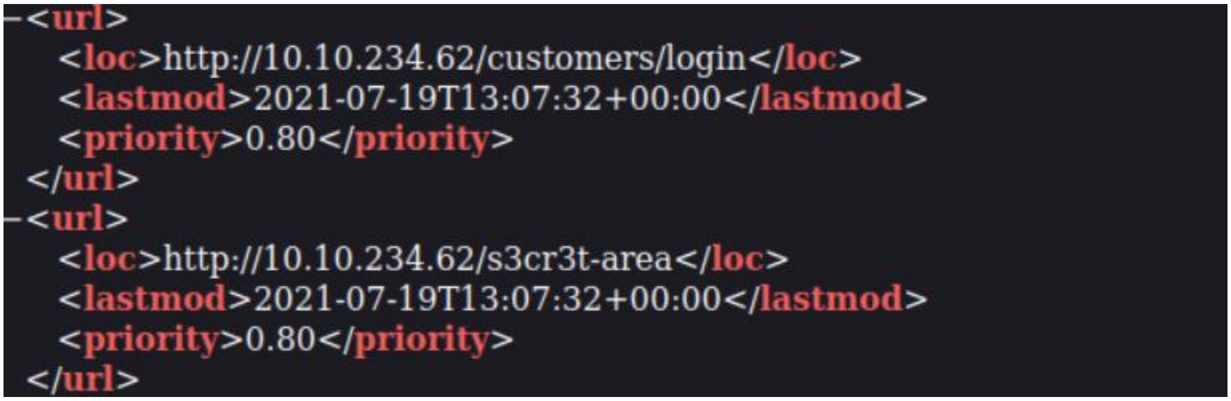
```
032ecc47c22a91e7f3f1d28a45d7f7bc:Ant docs (1.7.1) / libjakarta-
poi-java (3.0.2)
31aa07fe236ee504c890a61d1f7f0a97:apache2 (2.2.9) docs-manual
c0c4e7c0ac4da24ab8fc842d7f96723c:xsp (1.9.1)
d6923071afcee9cebcebc785da40b226:autopsy (2.08)
7513f4cf4802f546518f26ab5cfa1cad:axyl (2.6.0)
de68f0ad7b37001b8241bce3887593c7:b2evolution (2.4.2)
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
27c3b07523efd6c318a201cac58008ba:cimg (1.2.0.1)
ae59960e866e2730e99799ac034eacf7:webcit (7.37)
2ab2aae806e8393b70970b2eaace82e0:couchdb (0.8.0-0.9.1)
ddd76f1cfe31499ce3db6702991cbc45:cream (0.41)
74120b5bbc7be340887466ff6cfe66c6:cups (1.3.9) - doc
abeea75cf3c1bac42bbd0e96803c72b9:doc-iana-20080601
```

Answer the questions below

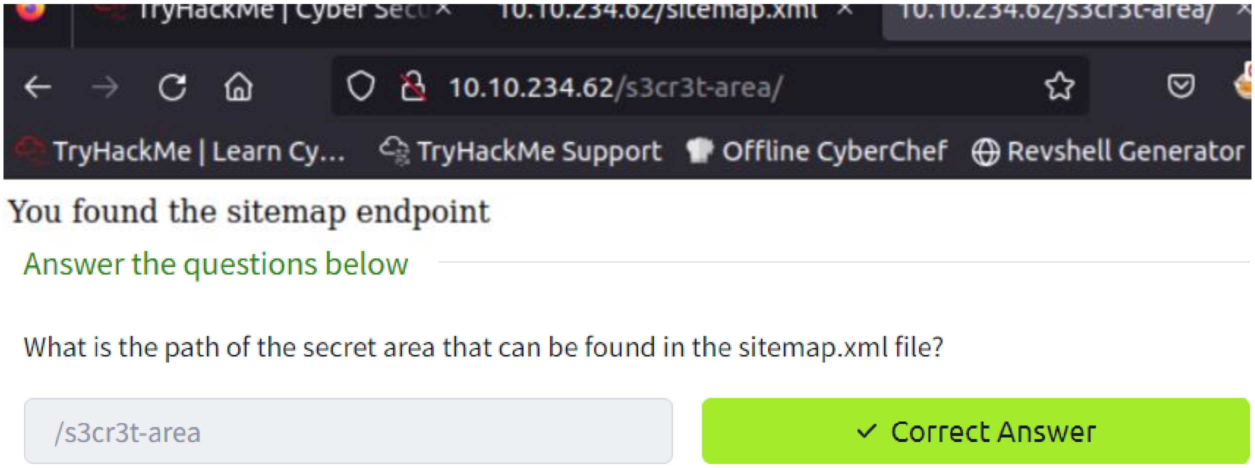
What framework did the favicon belong to?

cgiirc

Task 4:



```
<url>
  <loc>http://10.10.234.62/customers/login</loc>
  <lastmod>2021-07-19T13:07:32+00:00</lastmod>
  <priority>0.80</priority>
</url>
<url>
  <loc>http://10.10.234.62/s3cr3t-area</loc>
  <lastmod>2021-07-19T13:07:32+00:00</lastmod>
  <priority>0.80</priority>
</url>
```



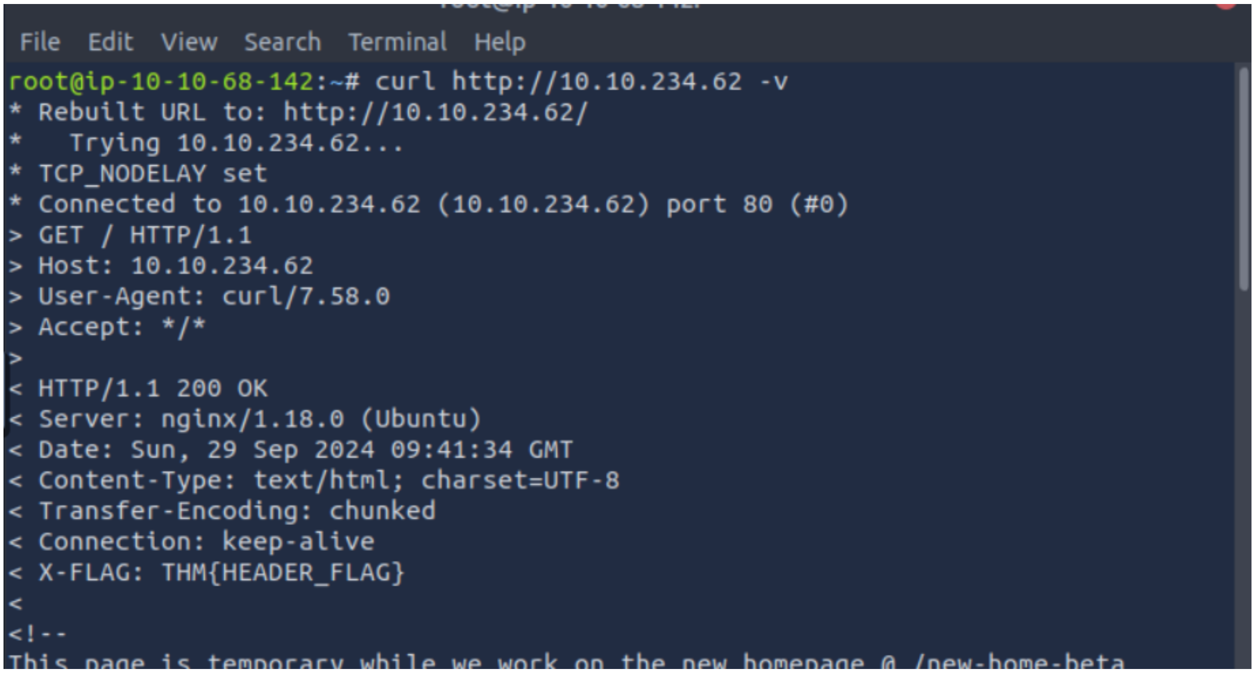
You found the sitemap endpoint

Answer the questions below

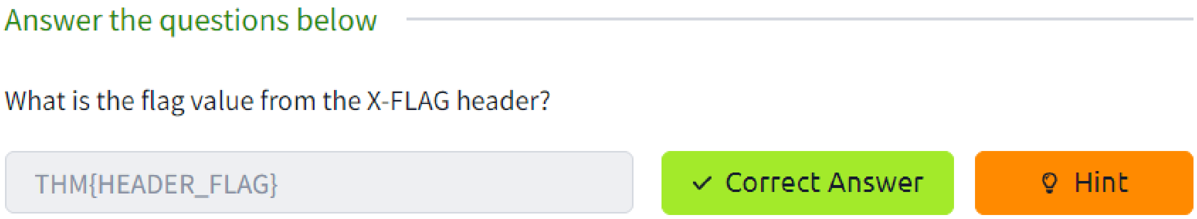
What is the path of the secret area that can be found in the sitemap.xml file?

/s3cr3t-area

Task 5:



```
root@ip-10-10-68-142:~# curl http://10.10.234.62 -v
* Rebuilt URL to: http://10.10.234.62/
*   Trying 10.10.234.62...
* TCP_NODELAY set
* Connected to 10.10.234.62 (10.10.234.62) port 80 (#0)
> GET / HTTP/1.1
> Host: 10.10.234.62
> User-Agent: curl/7.58.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: nginx/1.18.0 (Ubuntu)
< Date: Sun, 29 Sep 2024 09:41:34 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
```

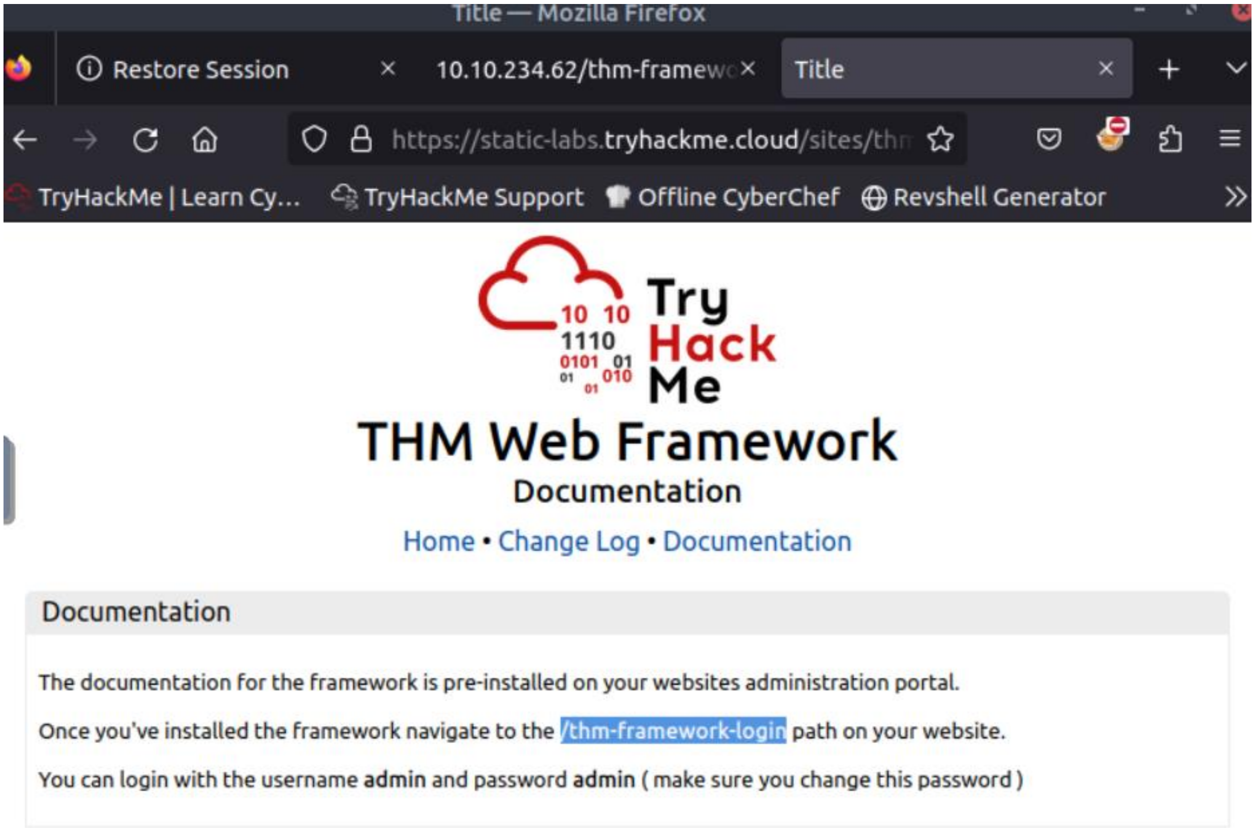


Answer the questions below

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

THM{HEADER_FLAG}

Task 6:



THM Web Framework

Documentation

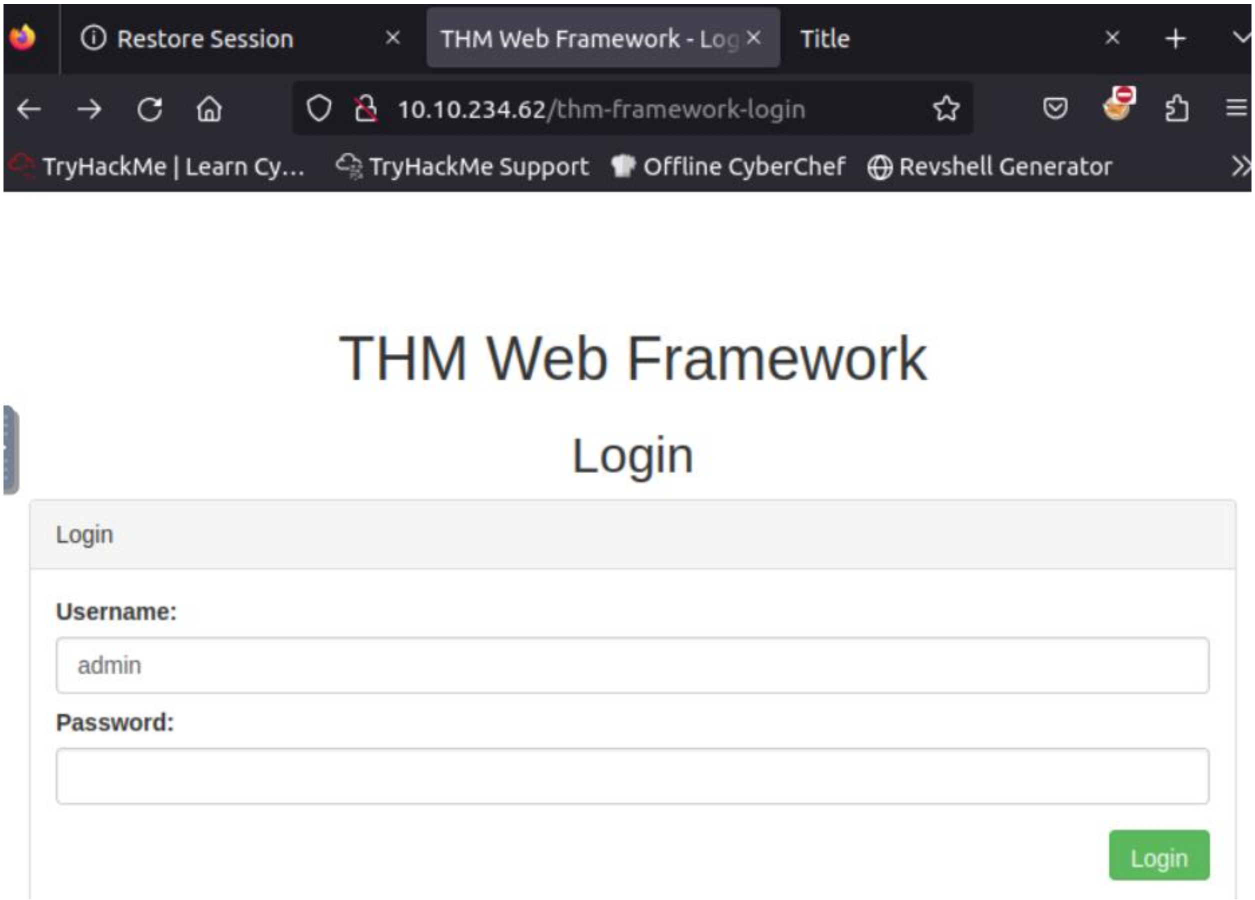
Home • Change Log • Documentation

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)



THM Web Framework

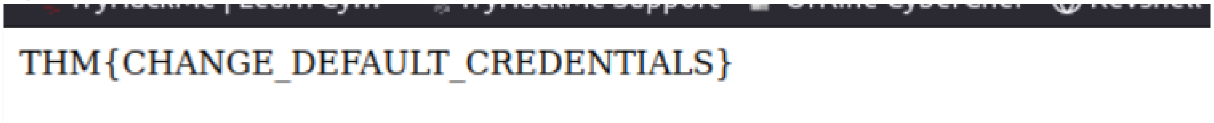
Login

Login

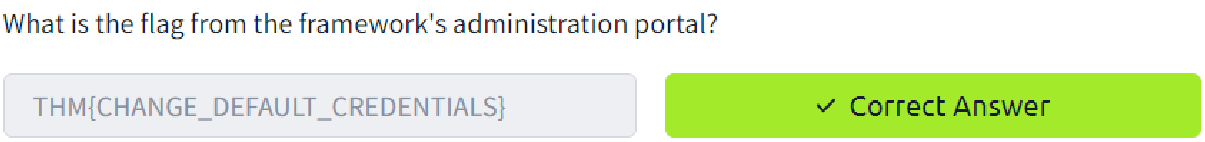
Username:

admin

Password:



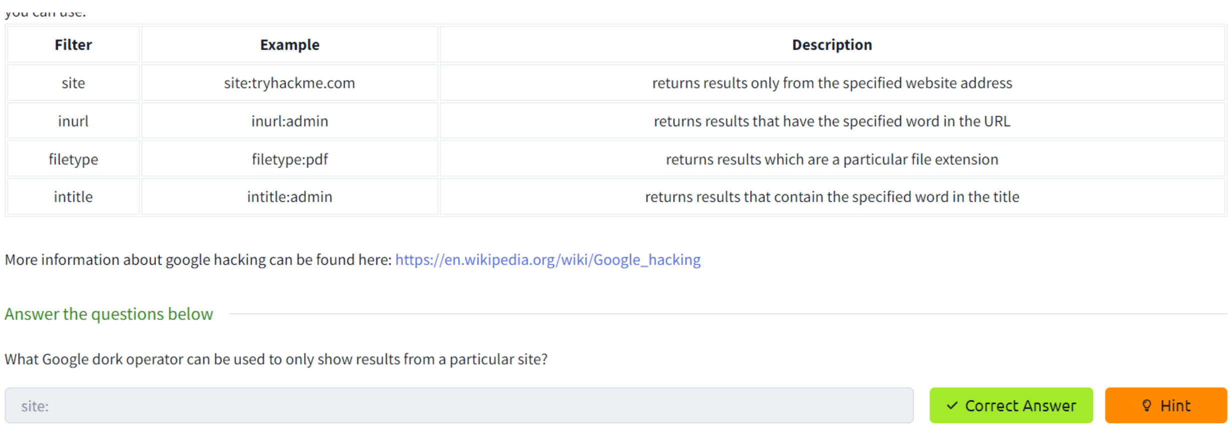
THM{CHANGE_DEFAULT_CREDENTIALS}



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

THM{CHANGE_DEFAULT_CREDENTIALS}

Task 7:



you can use.

Filter	Example	Description
site	site:tryhackme.com	returns results only from the specified website address
inurl	inurl:admin	returns results that have the specified word in the URL
filetype	filetype:pdf	returns results which are a particular file extension
intitle	intitle:admin	returns results that contain the specified word in the title

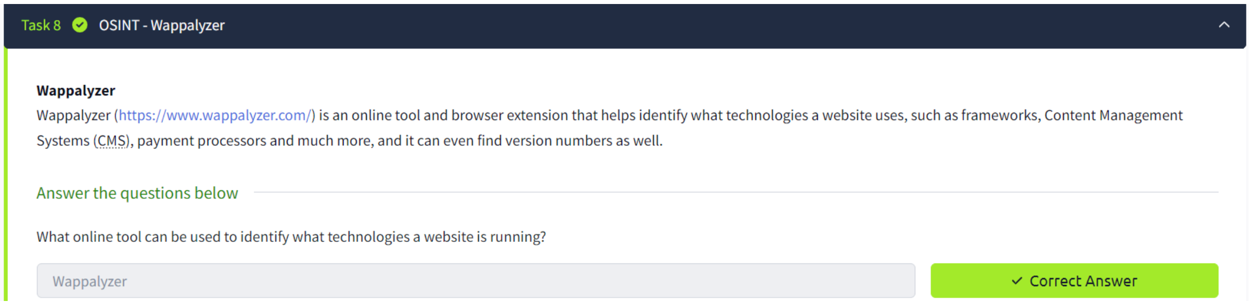
More information about google hacking can be found here: https://en.wikipedia.org/wiki/Google_hacking

Answer the questions below

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

site:

Task 8:



Task 8 ✓ OSINT - Wappalyzer

Wappalyzer

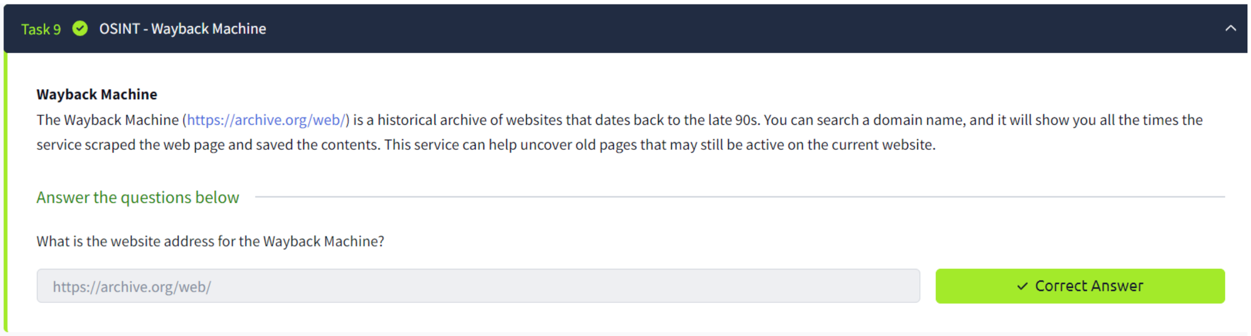
Wappalyzer (https://www.wappalyzer.com/) is an online tool and browser extension that helps identify what technologies a website uses, such as frameworks, Content Management Systems (CMS), payment processors and much more, and it can even find version numbers as well.

Answer the questions below

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

Wappalyzer

Task 9: https://archive.org/web/



Task 9 ✓ OSINT - Wayback Machine

Wayback Machine

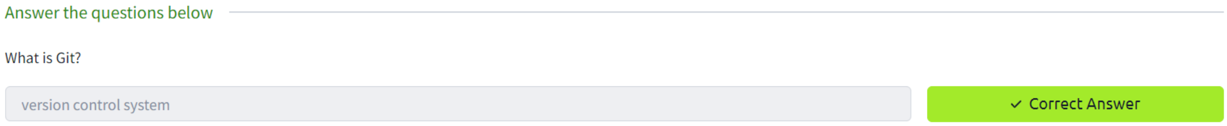
The Wayback Machine (https://archive.org/web/) is a historical archive of websites that dates back to the late 90s. You can search a domain name, and it will show you all the times the service scraped the web page and saved the contents. This service can help uncover old pages that may still be active on the current website.

Answer the questions below

What is the website address for the Wayback Machine?

https://archive.org/web/

Task 10:

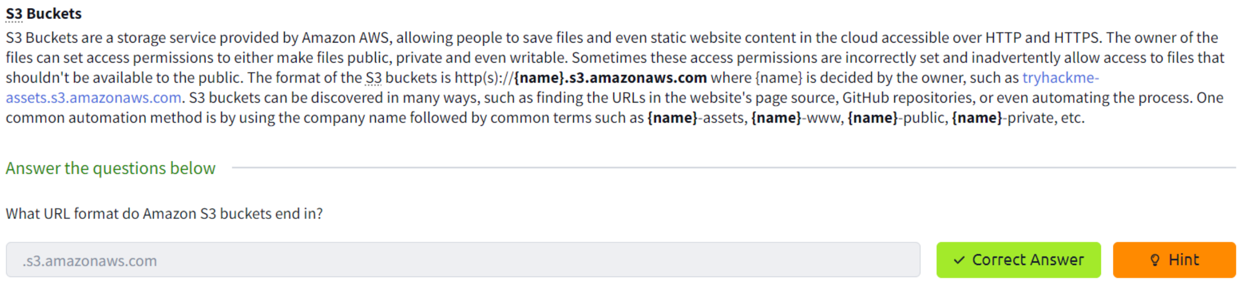


Answer the questions below

What is Git?

version control system

Task 11:



S3 Buckets

S3 Buckets are a storage service provided by Amazon AWS, allowing people to save files and even static website content in the cloud accessible over HTTP and HTTPS. The owner of the files can set access permissions to either make files public, private and even writable. Sometimes these access permissions are incorrectly set and inadvertently allow access to files that shouldn't be available to the public. The format of the S3 buckets is http(s)://**{name}.s3.amazonaws.com** where {name} is decided by the owner, such as tryhackme-assets.s3.amazonaws.com. S3 buckets can be discovered in many ways, such as finding the URLs in the website's page source, GitHub repositories, or even automating the process. One common automation method is by using the company name followed by common terms such as **{name}**-assets, **{name}**-www, **{name}**-public, **{name}**-private, etc.

Answer the questions below

What URL format do Amazon S3 buckets end in?

.s3.amazonaws.com