

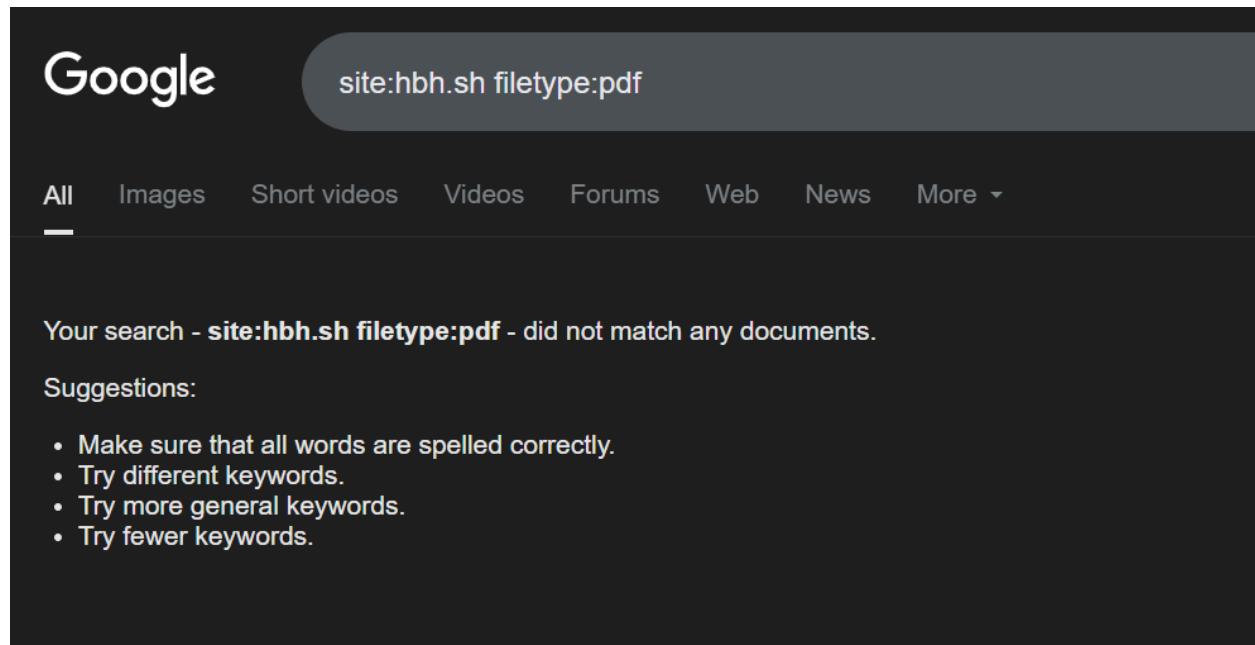
## Module 2\_ Assignment 1:

**Topic:** Gather information of a website using advanced google search and different tools.

Chosen Site: <https://hbh.sh/home>

**Purpose:** To identify any publicly available PDF files on the site.

**Result:** PDF not found.



**Purpose:** To search for login-related URLs.

**Result:** Found multiple URLs related to login pages.

Google site:hbh.sh inurl:login

All Images Videos Short videos Web News Forums More ▾

Gmail Hotmail Email Sportybet Yahoo PayPal Instagram

hbh.sh  
https://hbh.sh › forum › php-login ⋮

### PHP Login - Programming Thread | HBH

I'm trying to code a login for my site. It is an odd registration message whereby the regist send me an e-mail to check before I manually add the user ...

hbh.sh  
https://hbh.sh › index.php › auto-login-and-read-url-co... ⋮

### Auto login and read url content - PHP Code Bank - HBH

Sample code in PHP to login to a site like www.hellboundhackers.org and get contents

**Purpose:** To detect if the site exposes any email addresses

**Result:** Found multiple URLs related to gmail pages.

Google site:hbh.sh intext:@gmail.com

All Images Short videos News Videos Web Forums More ▾ Tools ▾

hbh.sh  
https://hbh.sh › code › python ⋮

### Python Code Bank | HBH

Welcome to HBH! If you have tried to register and didn't get a verification email, please using the following link to resend the verification email. Code Bank.

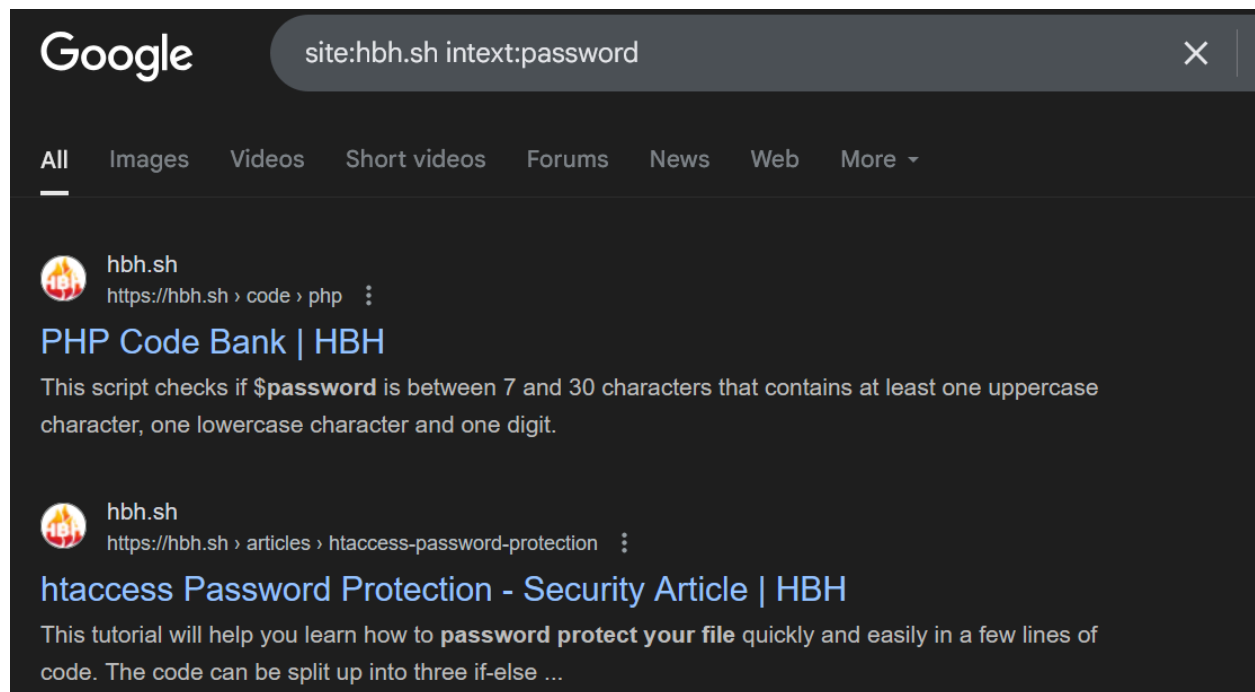
hbh.sh  
https://hbh.sh › forum › all-teams-looking-for-1-on-1-c... ⋮

### All teams, looking for 1 on 1 challenge - Teams Thread | HBH

DCS is ready: our site is live and our members are ready. contact [textdocument@gmail.com](mailto:textdocument@gmail.com) for a one on one duel between your team and DCS.

**Purpose:** To check if the word "password" is found anywhere on public pages.

**Result:** Found multiple URLs related to keyword pages.



**For gathering more information I have used ZoomEye website:**

Initially, I planned to use Shodan.io to gather information about the target website's server, open ports, and vulnerabilities. However, due to technical issues .such as the site not appearing in Shodan's database or failing to load properly .I was unable to retrieve the necessary data.

As a result, I used an alternative and powerful search engine called ZoomEye, which offers similar capabilities and is widely used in cybersecurity for information gathering.

More information for <https://hbh.sh/home>:

ResultReportMaps

Only \$10Download All

hellboundhackers.org:80

80http

hellboundhac...

>

Data update

HeaderBodyHash

United States

Organization: Cloudflare, Inc.

ASN: AS13335

Title: HBH: Learn how hackers bre...

🕒 2025-05-24 19:42

HTTP/1.1 301 Moved Permanently

Date: Sat, 24 May 2025 11:37:56 GMT

Content-Type: text/html

Content-Length: 167

Connection: keep-alive

Cache-Control: max-age=3600

Expires: Sat, 24 May 2025 12:37:56 GMT

Location: https://hellboundhackers.org/

Report-To: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report

NEL: {"success\_fraction":0,"report\_to":"cf-nel","max\_age":604800}

Vary: Accept-Encoding

X-Content-Type-Options: nosniff

Server: cloudflare

CF-RAY: 844-83100-f2f500f4-FRA

Copy

Show All

🕒 2025-05-19 19:31

Server: cloudflare

CF-RAY: 942344bcac5f2ab0-LAX

alt-svc: h3=":443"; ma=86400

server-timing: cfl4;desc="?proto=TCP&rtt=200317&min\_rtt=200314&rtt\_var=

hbh.sh:443

443https

hbh.sh

>

Data update

HeaderBodySSLHash

United States

Organization: Cloudflare, Inc.

ASN: AS13335

Title: HBH: Learn how hackers bre...

🕒 2025-05-19 19:30

HTTP/1.1 200 OK

Date: Mon, 19 May 2025 11:30:04 GMT

Content-Type: text/html; charset=UTF-8

Transfer-Encoding: chunked

Connection: keep-alive

Server: cloudflare

X-Content-Type-Options: nosniff

Cf-Ray: 9423429aebd3bbcb-FRA

Vary: Accept-Encoding

Cache-Control: no-cache, private

Content-Encoding: gzip

Access-Control-Allow-Origin: https://\*.hbh.sh

Cf-Cache-Status: DYNAMIC


## Attempt to Use Censys:

Initially, I attempted to use **Censys** (censys.io) to gather information about the target domain <https://hbh.sh/home> I used both domain-based and IP-based searches. However, Censys returned **no results**, which likely means that the domain or its IP address has not been scanned or indexed in their database.

## Alternative Approach:

Due to the lack of data in Censys, I decided to use an alternative open-source intelligence tool — **Whois.com** — which provided valuable information about the target server: Here some screen shorts:

# hbh.sh

 Domain Information	
Domain:	hbh.sh
Registered On:	2020-07-28
Expires On:	2026-07-28
Updated On:	2025-03-03
Status:	clientTransferProhibited
Name Servers:	james.ns.cloudflare.com elma.ns.cloudflare.com

## Registrar Information

Registrar:	Cloudflare, Inc
IANA ID:	1910
URL:	<a href="http://cloudflare.com">http://cloudflare.com</a>
Abuse Email:	<a href="mailto:registrar-notices@cloudflare.com">registrar-notices@cloudflare.com</a>

## Registrant Contact

State:	Lancashire
Country:	GB

## Raw Whois Data

Domain Name: hbh.sh  
Registry Domain ID: 9fd3e884ec38421c876ffacef74f56b7-DONUTS  
Registrar WHOIS Server: <http://whois.cloudflare.com>  
Registrar URL: <http://cloudflare.com>  
Updated Date: 2025-03-03T17:29:47Z  
Creation Date: 2020-07-28T08:55:23Z  
Registry Expiry Date: 2026-07-28T08:55:23Z  
Registrar: Cloudflare, Inc  
Registrar IANA ID: 1910  
Registrar Abuse Contact Email: [registrar-notices@cloudflare.com](mailto:registrar-notices@cloudflare.com)  
Registrar Abuse Contact Phone:  
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>  
Registry Registrant ID: REDACTED  
Registrant Name: REDACTED  
Registrant Organization:  
Registrant Street: REDACTED  
Registrant City: REDACTED  
Registrant State/Province: Lancashire  
Registrant Postal Code: REDACTED  
Registrant Country: GB

In conclusion, this reconnaissance assignment provided a practical understanding of how to extract valuable information about a target using these tools. While Censys did not return any results for the target domain/IP, alternative tools such as ZoomEye and [Whois.com](https://whois.com/whois/) were effectively used to gather technical data including open ports, services, SSL details, and host metadata.

This experience highlighted the importance of using multiple tools during reconnaissance, as each may yield different results depending on their scanning coverage. By adapting to the challenges (such as tool limitations), I was able to complete the task successfully using some alternatives and analytical reasoning.