



HellboundHackers (hbh.sh)

Ethical Hacking, System Protection, and Web Vulnerability Detection

SYNOPSIS

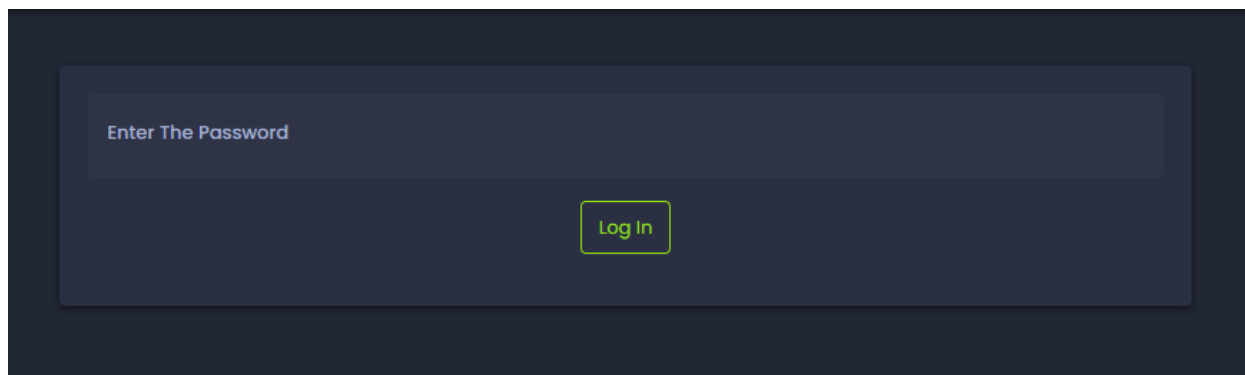
HBH was founded in 2003 as a place to learn how hackers break in, how to protect your systems and a place to share information freely. Now 20 years later HBH is a non-profit with over 152 simulated challenges and virtual machine based labs with real world system and vulnerabilities.

GOAL

The goal of teaching everyone the best practices for security and the new methods and tactics used by black hats, HBH aims to keep you and your team up to date with the latest advances in infosec.

Confirmed Vulnerabilities


#1 Source Code Inspection for the hidden password



```

    </div>
  </div>
</div>
<div class="row pt-3 align-items-center">
  <div class="col-6 mx-auto">
    <div class="card">
      <div class="card-body text-center">
        <!-- f6Nkw1ZbdfQhp -->
        <form method="POST" action="https://hbh.sh/challenges/prerequisites/1" autocomplete="off">
          <input type="hidden" name="_token" value="YgxHhKX99NNkrsGuhV5YPAlM2Tvej2ra23Pv094u">
          <div class="form-floating mb-3">
            <input type="text" class="form-control" id="floatingPassword" name="password" placeholder="Enter The Password" data-lpignore="true">
            <label for="floatingPassword">Enter The Password</label>
          </div>
          <div class="form-group mb-3">
            <button class="btn btn-outline-success waves-effect waves-light" type="submit">Log In</button>
          </div>
        </form>
      </div>
    </div>
  </div>
</div>
</div>
</div>
</div>
<div>
  <div class="footer" style="height: 70px!important;">
    <div class="container-fluid">
      <div class="row">
        <div class="col-sm-6">
          &copy; 2022 HBH - Version <a href="https://hbh.sh/development/changelog">2.0.13</a>

```



Congrats!

You have completed Prerequisite 1

As such 5 points have been added to your account.

Progress to the next challenge →

i

Explanation

This challenges aim is to get you into the habit of view the source of a page. Hopefully in most cases a password would never be in the source code for page but it can provide you some helpful insights into an application and may help on the discovery of more entry points. Why not have a look over our source code and see if you can find anything ?

#2 Source code inspections for the URL hidden inside the web page

```

<div class="align-self-center">
  <p class="font-size-18">
    <i class='fal fa-biohazard'></i> Prerequisite 2
  </p>
</div>
<div class="p-2">
  <a href="https://hbb.sh/challenges/prerequisites/3">Next Challenge <i class='fal fa-arrow-right'></i></a>
</div>
</div>
</div>
</div>
<div class="row pt-3 align-items-center">
  <div class="col-6 mx-auto">
    <div class="card">
      <div class="card-body text-center">
        <p class="text-muted">
          My friend Drake has begin to program in HTML and he made this IFRAME, but the host of the website has kicked him out, and he doesnt remember where is this IFRAME reading it from.
        </p>
        <iframe height="80%" width="80%" src="https://hbb.sh/challenges/pw420m71u/iframe"></iframe>
        <hr>
        <p class="text-muted">Please submit the full URL that the IFRAME is reading from using the form below.</p>
        <form method="POST" action="https://hbb.sh/challenges/prerequisites/2" autocomplete="off">
          <input type="hidden" name="token" value="y2U8qneDy5NqXkXbCKEhUhcJ9nTCPiEuUhd1ZizP">
          <input type="text" class="form-control" id="floatingPath" name="path" placeholder="IFRAME Path" data-lpignore="true">
          <label for="floatingPath">IFRAME Path</label>
        </div>
        <div class="form-group mb-3">
          <button class="btn btn-outline-success waves-effect waves-light" type="submit">Send path to Drake</button>
        </div>
      </div>
    </div>
  </div>
</div>

```

My friend Drake has begin to program in HTML and he made this IFRAME, but the host of the website has kicked him out, and he doesnt remember where is this IFRAME reading it from.


Welcome to my first IFRAME page

I have just found out how to use an IFRAME

Please submit the full URL that the IFRAME is reading from using the form below.

IFRAME Path

Send path to Drake



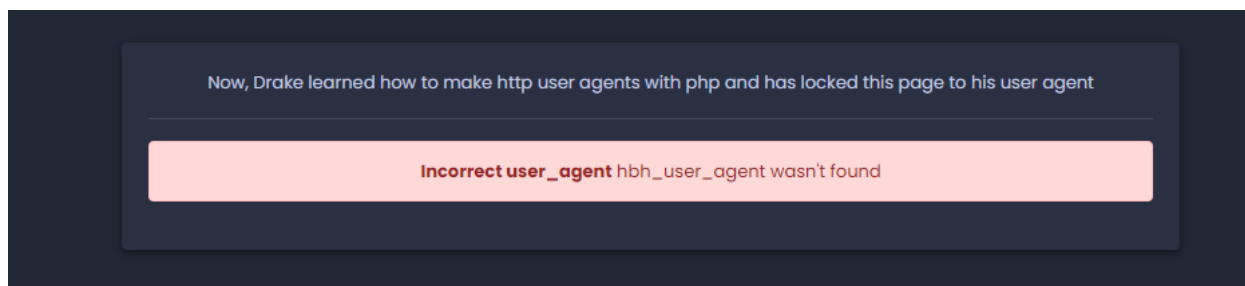
Congrats!

You have completed Prerequisite 2

However as you have completed this challenge before no points will be awarded.

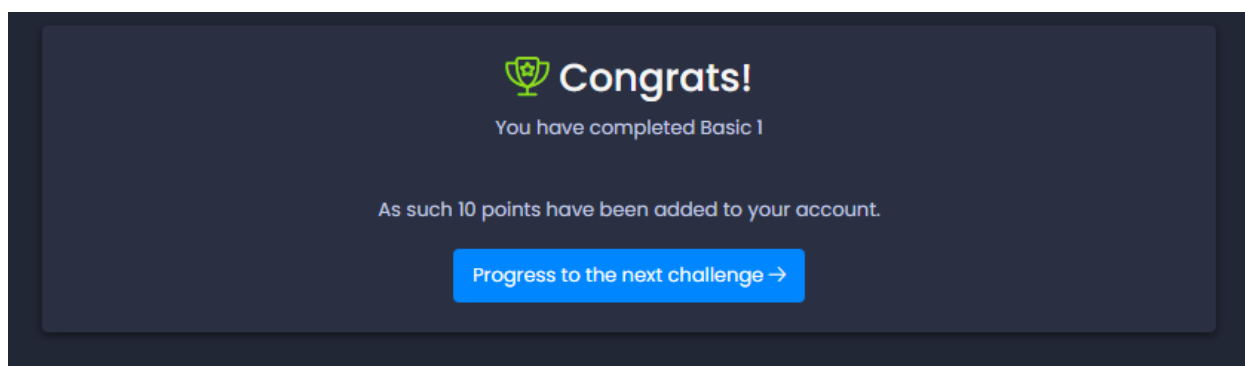
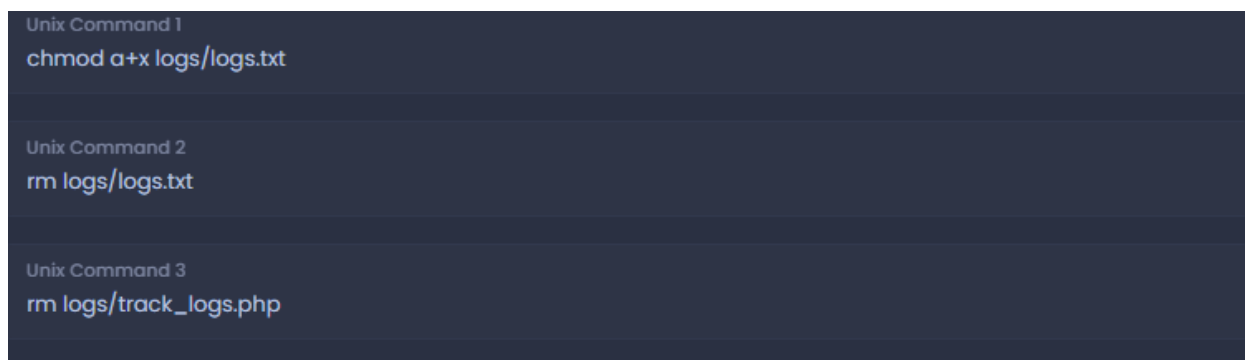
Progress to the next challenge →

#3



According to developer.mozilla.org, it is a characteristic string that lets servers and network peers identify the application, operating system, vendor and/or version of the requesting user_agent. To solve this, I need to switch agents to hbh_user_agent. It basically gives certain criteria for certain users in the sense that if those criteria are not met, then the page would not load and display the proper information. To solve this, I have to switch to a different agent using the above hbh_user_agent to enable content for this page. Since I do not want to download the software or plugin for this, I'll only state it in this sentence.

#4 Inspection of the php file showed 2 files, only thing to do is use the proper code according to the instruction



#5 Using wildcards to get information on the login page and from the error it gave after trying different special characters


Welcome to Asterix-Protect Asterix-Protect is an email search system that uses this new type of Asterix database to match your search and uses the same type of form like a login. And Asterix-Protect its a login system which also uses this advanced type Asterix database to match your username;password, this is a project that just started... If something is wrong or you have found a bug in our product, please contact us at problems@Asterix-Protect.org.

Enter Username:Password
@:

Login

Search an E-mail


Search

 **Congrats!**
You have completed Basic 2

As such 10 points have been added to your account.

[Progress to the next challenge →](#)

#6 After trying some passwords, SQL Query Error showed the SQL syntax that would enable hackers to use the SQL string by doing a URL tamper.

 https://hbh.sh/challenges/basic/4?sql_query=SELECT * FROM family_db

This time Drake invented a secure PHP and MySQL login, so only his family can login, but the script wasn't as secure as he thought it would be.

Your password is KingKong

Username

Drake

Password

KingKong

Login



Congrats!

You have completed Basic 4

However as you have completed this challenge before no points will be awarded.

[Progress to the next challenge →](#)

#7 Use poison null byte to be able to access page without login

Search for Files

With this file search engine, you can search files only on the folder **files** which your administrator has set up for you to search. You can search anything in **files** and if your search was matched then it would show you the content of that file

Search

Login

hbk.sh/challenges/basic/5/files

Index of /files

Name	Last modified	Size	Description
<hr/>			
Parent Directory	-		
login.php	2022-03-30 02:23	127	
search.php	2022-03-30 02:23	127	

Search for Files

With this file search engine, you can search files only on the folder **files** which your administrator has set up for you to search. You can search anything in **files** and if your search was matched then it would show you the content of that file

login.php%00

Search

```
<div class="row pt-3 align-items-center">
  <div class="col-6 mx-auto">
    <div class="card">
      <p class="card-body text-center">
        <p class="text-muted"><script language='JavaScript' type='ea094d8eaf06125d4b62787b-text/javascript"><Hide this Information: Password == environment & Username == FastLane</script></p>
      </div>
    </div>
  </div>
</div>
```

Search for Files

With this file search engine, you can search files only on the folder **files** which your administrator has set up for you to search. You can search anything in **files** and if your search was matched then it would show you the content of that file

Search
login.php%00

Search

Username
FastLane

Password
environment

Login



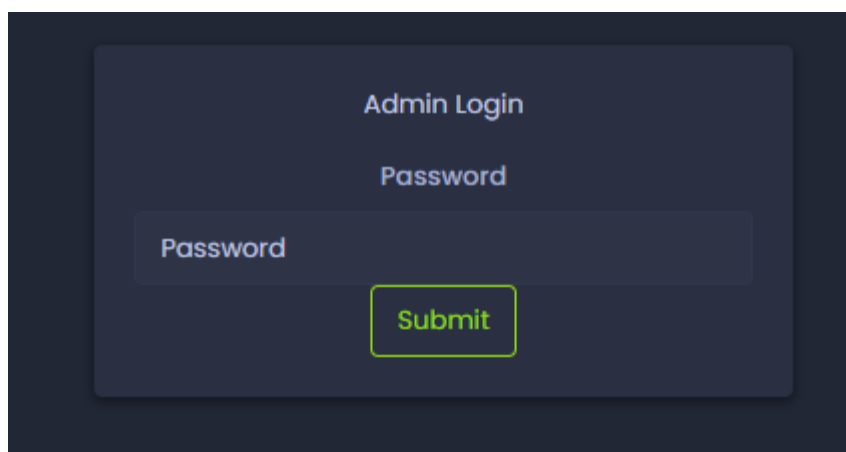
Congrats!

You have completed Basic 5

As such 20 points have been added to your account.

[Progress to the next challenge →](#)

#8 Looked at the source code and found a comment saying to look at /newpasswd/admin.txt

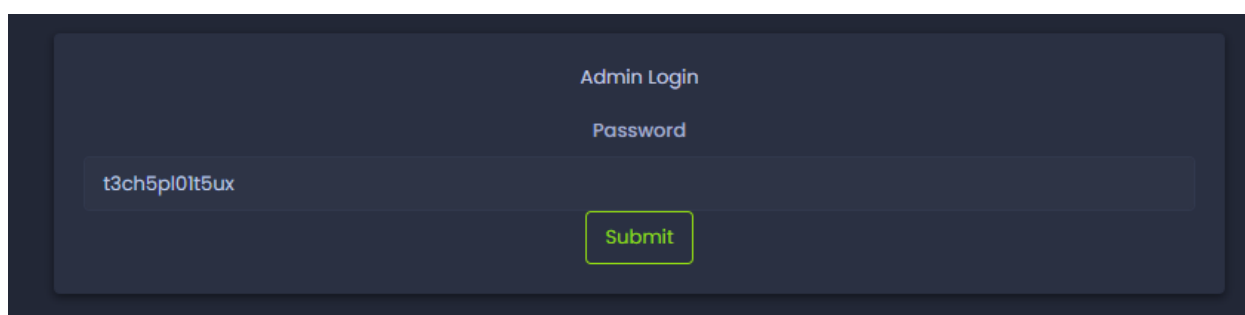


Admin Login

Password

Password

Submit



Admin Login

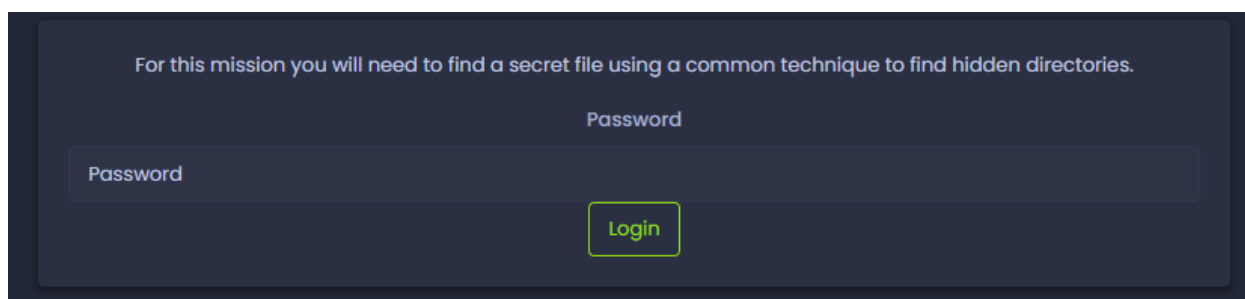
Password

t3ch5pl0t5ux

Submit

#9

Using the robots.txt file to find the hidden file and hint was given inside the source code.



For this mission you will need to find a secret file using a common technique to find hidden directories.

Password

Password

Login

```
User-agent: *  
Disallow: abc/hidden.txt
```

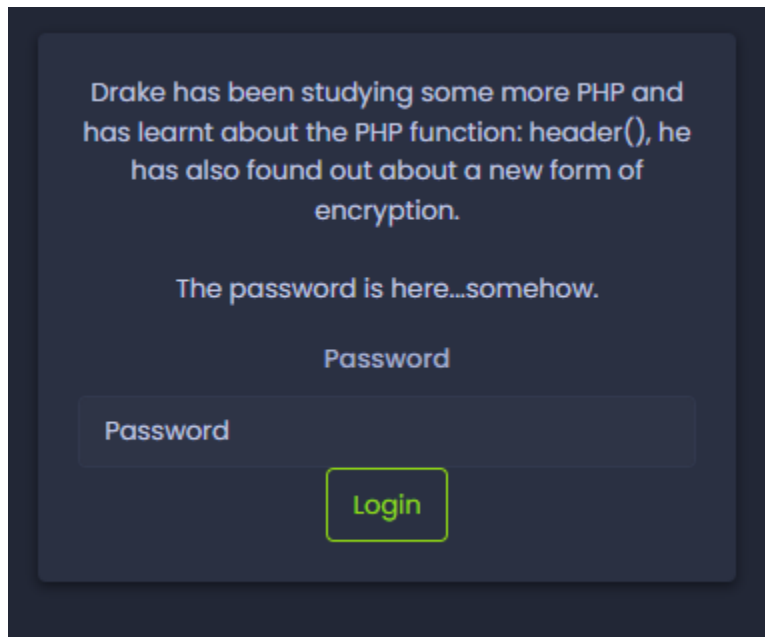
welldone, you have found the hidden file.

robots.txt is a very common method for webmasters to stop search engines from searching certain folders.

To find out more about robots.txt do a quick google search.

THE PASSWORD FOR THE CHALLENGE IS: heavenbound

#10 Inspect page and check the networks tab. I looked for the php file from the “14” (this was done after trying to inspect everything from the webpage to the cookies and nothing). Decoding the password found by using Rot47 as the cipher.



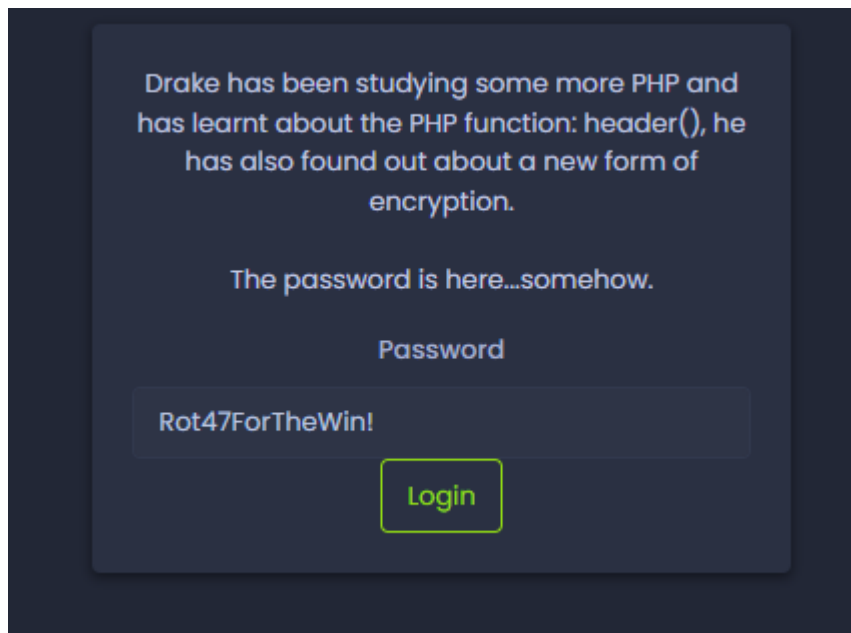
Drake has been studying some more PHP and has learnt about the PHP function: `header()`, he has also found out about a new form of encryption.

The password is here...somehow.

Password

Password

Login



Drake has been studying some more PHP and has learnt about the PHP function: `header()`, he has also found out about a new form of encryption.

The password is here...somehow.

Password

Rot47ForTheWin!

Login

cookie-domain:hbh.sh cook

5000 ms 10000 ms 15000 ms 20000 ms 25000 ms 30000 ms 35000 ms 40000 ms 45000 ms 50000 ms 55000 ms

Name Headers Preview Response Initiator Timing Cookies

14

livewire.js?id=940557fc56b15...
app.min.js?id=b3120411f97df...
chat.js
cookies.js
node-waves.min.js?id=16995...
simplebar.min.js?id=f92507da...
metismenu.min.js?id=90334a...
bootstrap.min.js?id=bb2ab2f5...
jquery.min.js?id=8fb8fee4fcc3...
funding.js
prism.js
favicon.ico
favicon.ico
hbh-logo.svg
rum
rum

17 / 41 requests | 8.9 kB / 11.9 kB

General

Request URL: <https://hbh.sh/challenges/basic/14>
Request Method: GET
Status Code: 200
Remote Address: 172.67.150.93:443
Referrer Policy: strict-origin-when-cross-origin

Response Headers

access-control-allow-origin: https://*.hbh.sh
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
cache-control: no-cache, private
cf-cache-status: DYNAMIC
cf-ray: 6f3f1825af437cb9-LAX
content-encoding: br
content-type: text/html; charset=UTF-8
date: Wed, 30 Mar 2022 07:22:28 GMT
encryption: ROT-47
expect-ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
password: #@EcFu@C%96(:?P
report-to: {"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v3?s=kHRT5EyOZ6BrXCUAP4gD6tbd1IT15FL0t6Q4WkrvkysEDqBQNFm3jP3%2BUGKasecpxp1N%2F17d3w0ecA%2Fj%2FvDMDKdU%2BvUEQR1aoYzH%2BfILr2IvEYEEc51tVRA%3D"}],"group":"cf-nel","max_age":604800}

Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'sudoku'

★ BROWSE THE [FULL DCODE TOOLS' LIST](#)

Results

Rot47ForTheWin!
ROT-47 Cipher - [dCode](#)
Tag(s) : Substitution Cipher, Internet

Share

+

f

Twitter

Reddit

Envelope

ROT-47 CIPHER

Cryptography › Substitution Cipher › ROT-47 Cipher

ROT47 DECODER

★ ROT47 CIPHERTEXT

#@EcFu@C%96(:?P

▶ DECRYPT ROT47

See also: [ROT Cipher](#) – [ROT-13 Cipher](#) – [Caesar Cipher](#)

ROT47 ENCODER

★ CAESAR CODE PLAIN TEXT

dCode Rot-47