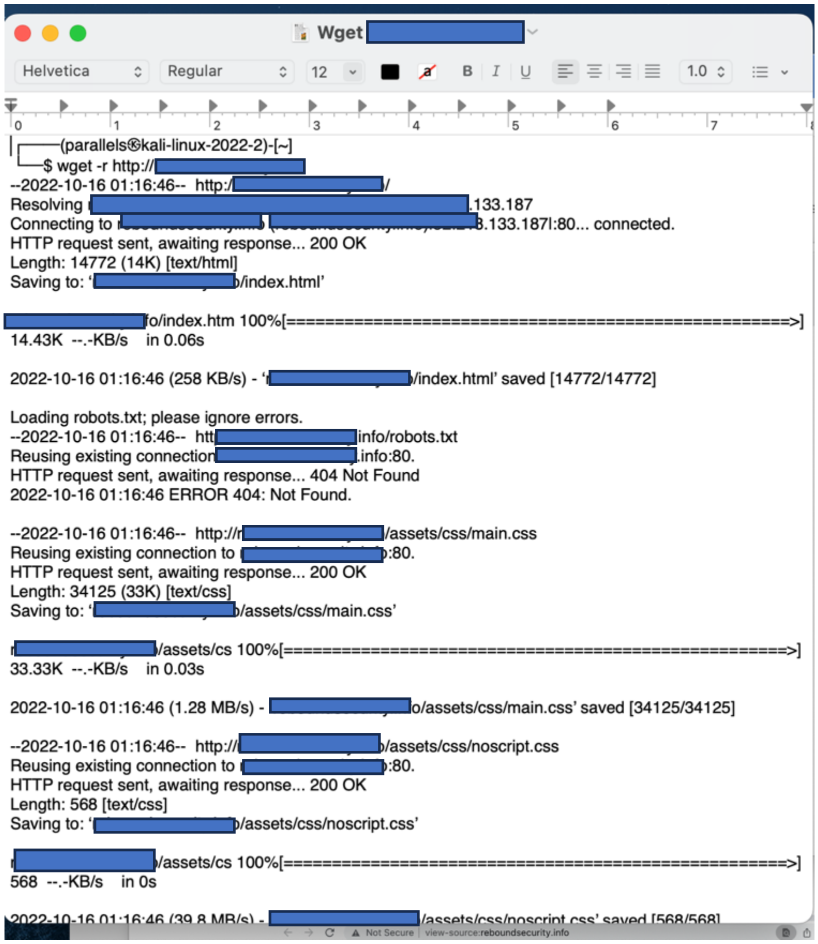
Jorael Jamison
CSIA320
Professor Eric Robinson
10/18/2022

Exam – Capture the Flags 1

/FLAG1/

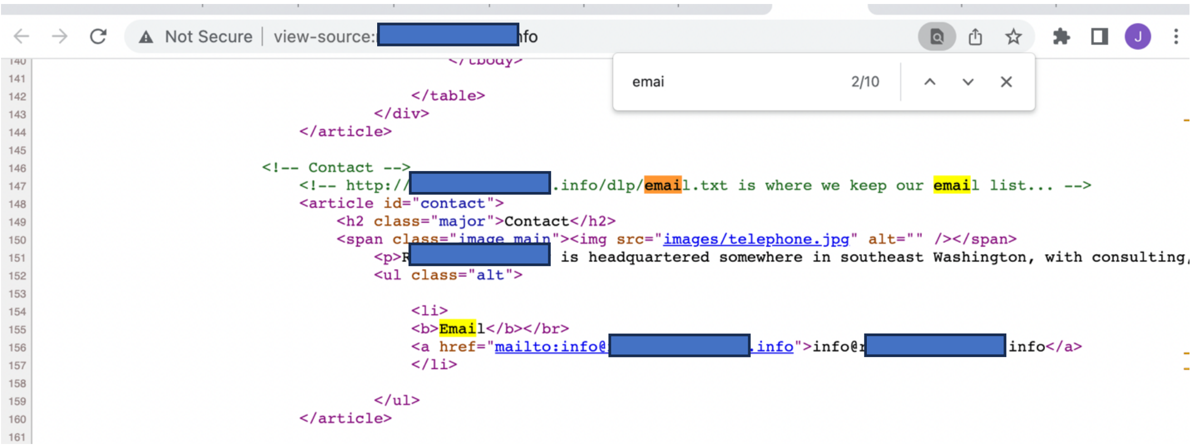
Used the Wget -r command and saved the results in a .txt file. Nothing found within this file of use for this step.



```
┌──(parallels㉿kali-linux-2022-2)-[~]
└─$ wget -r http://[redacted]
--2022-10-16 01:16:46--  http:/[redacted]/
Resolving [redacted].133.187
Connecting to [redacted] ([redacted].133.187|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14772 (14K) [text/html]
Saving to: '[redacted]/index.html'

[redacted]o/index.htm 100%[====================================================>]
 14.43K  --.-KB/s    in 0.06s

2022-10-16 01:16:46 (258 KB/s) - '[redacted]/index.html' saved [14772/14772]

Loading robots.txt; please ignore errors.
--2022-10-16 01:16:46--  htt[redacted]info/robots.txt
Reusing existing connection[redacted].info:80.
HTTP request sent, awaiting response... 404 Not Found
2022-10-16 01:16:46 ERROR 404: Not Found.

--2022-10-16 01:16:46--  http://[redacted]/assets/css/main.css
Reusing existing connection to [redacted]:80.
HTTP request sent, awaiting response... 200 OK
Length: 34125 (33K) [text/css]
Saving to: '[redacted]/assets/css/main.css'

[redacted]/assets/cs 100%[====================================================>]
 33.33K  --.-KB/s    in 0.03s

2022-10-16 01:16:46 (1.28 MB/s) - [redacted]o/assets/css/main.css' saved [34125/34125]

--2022-10-16 01:16:46--  http://[redacted]/assets/css/noscript.css
Reusing existing connection to [redacted]:80.
HTTP request sent, awaiting response... 200 OK
Length: 568 [text/css]
Saving to: '[redacted]/assets/css/noscript.css'

[redacted]/assets/cs 100%[====================================================>]
 568  --.-KB/s    in 0s

2022-10-16 01:16:46 (39.8 MB/s) - [redacted]/assets/css/noscript.css' saved [568/568]
```

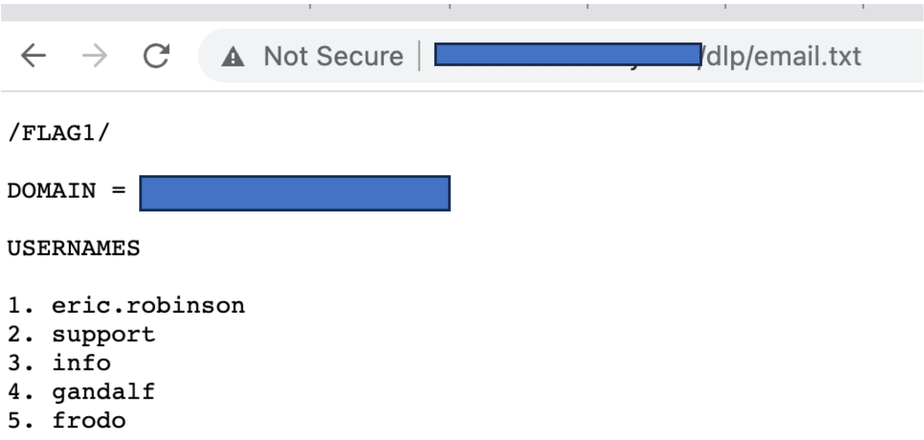
Next, I opened the Web site http://[redacted] and viewed the source code using Chrome. I searched for the keyword "email" and found a line showing:

http://[redacted]/dlp/email.txt is where we keep our email list... -->



```
                    </tbody>
                </table>
            </div>
        </article>

    <!-- Contact -->
        <!-- http://[redacted].info/dlp/email.txt is where we keep our email list... -->
        <article id="contact">
            <h2 class="major">Contact</h2>
            <span class="image main"><img src="images/telephone.jpg" alt="" /></span>
                <p>[redacted] is headquartered somewhere in southeast Washington, with consulting,
                <ul class="alt">

                    <li>
                    <b>Email</b></br>
                    <a href="mailto:info@[redacted].info">info@[redacted]info</a>
                    </li>

                </ul>
        </article>
```

I accessed that website, and it displayed the page below listing the usernames for [redacted] and /FLAG1/.



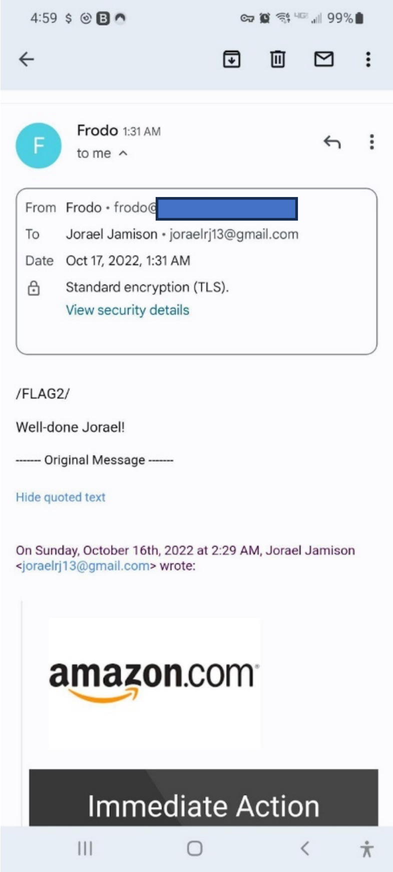
```
/FLAG1/

DOMAIN = [redacted]

USERNAMES

1. eric.robinson
2. support
3. info
4. gandalf
5. frodo
```

I took those usernames and added the "@domainName" at the end of each to make a full email address:

eric.robinson[redacted]
support@[redacted]
info@[redacted]
gandalf@[redacted]
frodo@[redacted]

/FLAG2/

I created a phishing Amazon email asking the victim to click yes or no to confirm a recent high-valued purchase was legitimate or not. This was individually sent to the five email addresses above. It gives them a sense of urgency that this high-valued purchase may be approved that they did not make, while concerned their account has been compromised. The email looks to be from a trusting source – Amazon. It has only two options both requiring a response yes or no which when clicked can re-direct to the Amazon site for login credentials or even have malware downloaded on their computer.



Frodo 1:31 AM
to me

From Frodo • frodo@[redacted]
To Jorael Jamison • joraelrj13@gmail.com
Date Oct 17, 2022, 1:31 AM
Standard encryption (TLS).
View security details

/FLAG2/

Well-done Jorael!

------- Original Message -------

Hide quoted text

On Sunday, October 16th, 2022 at 2:29 AM, Jorael Jamison <joraelrj13@gmail.com> wrote:

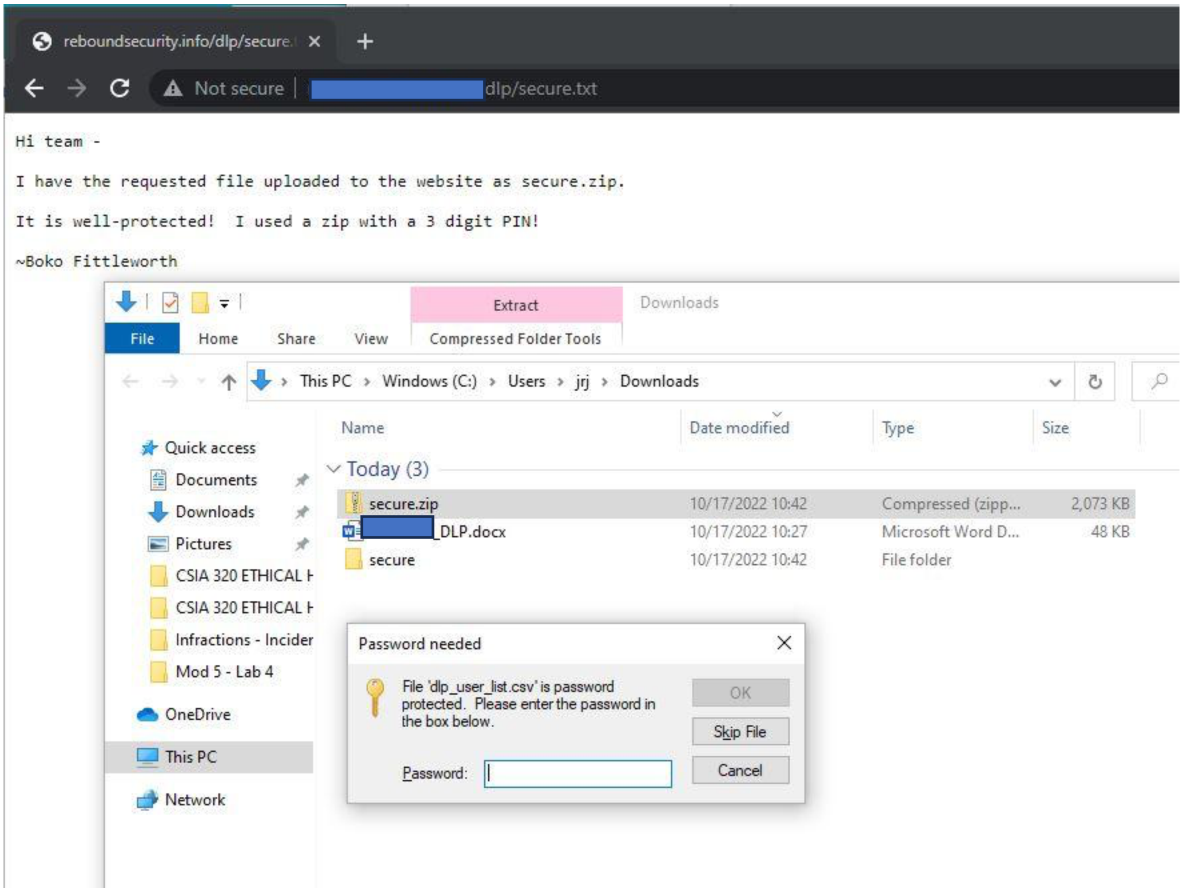
Above is the response back I received in my inbox and /FLAG2/.

/FLAG3/

User: 592367 from Legal Department.

On [redacted] under the DLP tab I selected “Read Me!”. It directed me to a page saying the requested file is a secure.zip file on the website - secured by a 3-digit pin. I typed the following into the browser and a secure.zip file was downloaded (password protected.)

[redacted]/dlp/secure.zip



```
Hi team -

I have the requested file uploaded to the website as secure.zip.

It is well-protected!  I used a zip with a 3 digit PIN!

~Boko Fittleworth
```

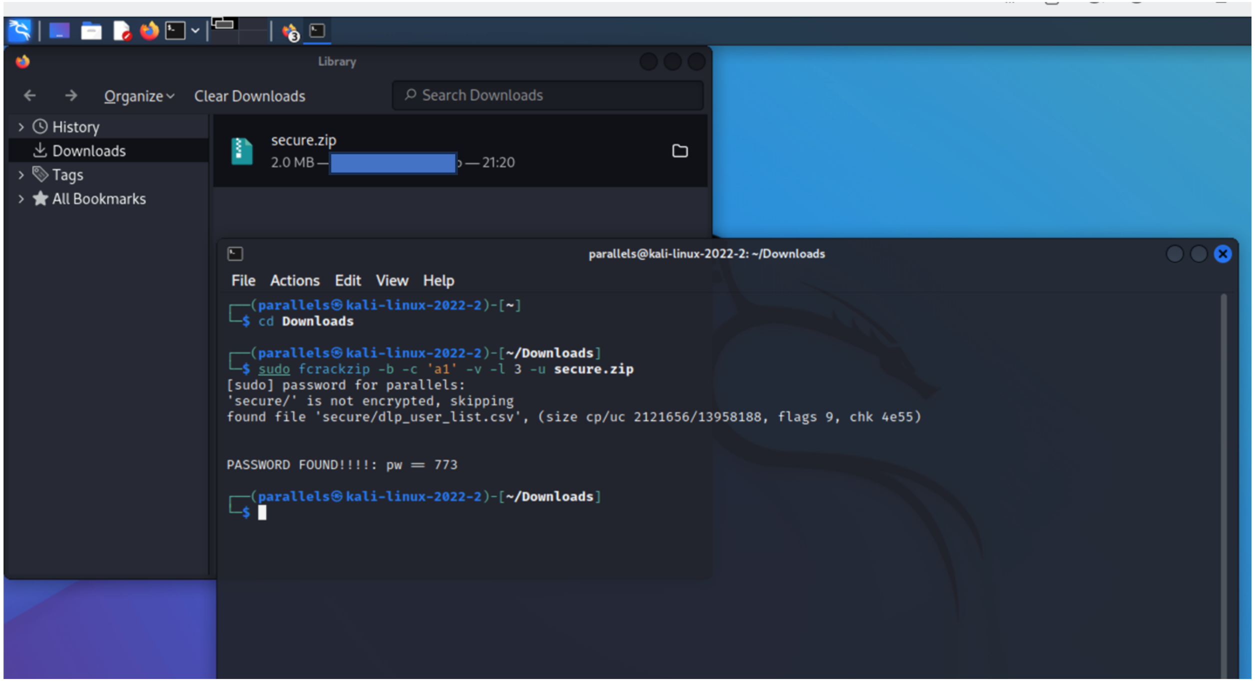
Name	Date modified	Type	Size
Today (3)			
secure.zip	10/17/2022 10:42	Compressed (zipp...	2,073 KB
[redacted] DLP.docx	10/17/2022 10:27	Microsoft Word D...	48 KB
secure	10/17/2022 10:42	File folder	

Password needed

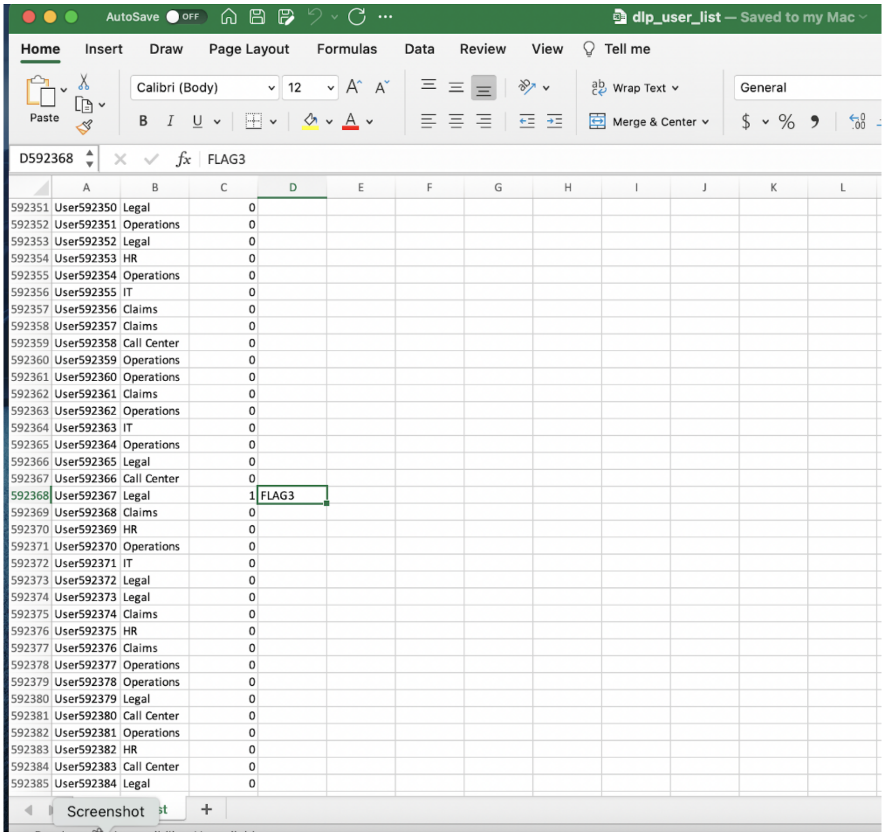
File 'dlp_user_list.csv' is password protected. Please enter the password in the box below.

Password:

I ran a series of cracking tools in Kali Linux from Hashcat, John the Ripper and fcrackzip until I was able to successfully crack the the secure.zip file. The program that worked easiest for me was *fcrackzip* and the Password = 773.



```
┌──(parallels㉿kali-linux-2022-2)-[~]
└─$ cd Downloads

┌──(parallels㉿kali-linux-2022-2)-[~/Downloads]
└─$ sudo fcrackzip -b -c 'a1' -v -l 3 -u secure.zip
[sudo] password for parallels:
'secure/' is not encrypted, skipping
found file 'secure/dlp_user_list.csv', (size cp/uc 2121656/13958188, flags 9, chk 4e55)


PASSWORD FOUND!!!!: pw == 773

┌──(parallels㉿kali-linux-2022-2)-[~/Downloads]
└─$ █
```



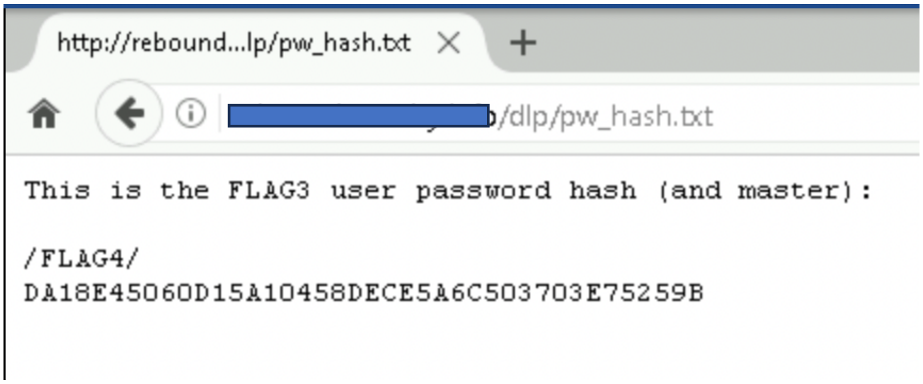
D592368 fx FLAG3

	A	B	C	D
592351	User592350	Legal	0	
592352	User592351	Operations	0	
592353	User592352	Legal	0	
592354	User592353	HR	0	
592355	User592354	Operations	0	
592356	User592355	IT	0	
592357	User592356	Claims	0	
592358	User592357	Claims	0	
592359	User592358	Call Center	0	
592360	User592359	Operations	0	
592361	User592360	Operations	0	
592362	User592361	Claims	0	
592363	User592362	Operations	0	
592364	User592363	IT	0	
592365	User592364	Operations	0	
592366	User592365	Legal	0	
592367	User592366	Call Center	0	
592368	User592367	Legal	1	FLAG3
592369	User592368	Claims	0	
592370	User592369	HR	0	
592371	User592370	Operations	0	
592372	User592371	IT	0	
592373	User592372	Legal	0	
592374	User592373	Legal	0	
592375	User592374	Claims	0	
592376	User592375	HR	0	
592377	User592376	Claims	0	
592378	User592377	Operations	0	
592379	User592378	Operations	0	
592380	User592379	Legal	0	
592381	User592380	Call Center	0	
592382	User592381	Operations	0	
592383	User592382	HR	0	
592384	User592383	Call Center	0	
592385	User592384	Legal	0	

Extracted the file dlp_user_list and did a word search for "flag" and found /FLAG3/.

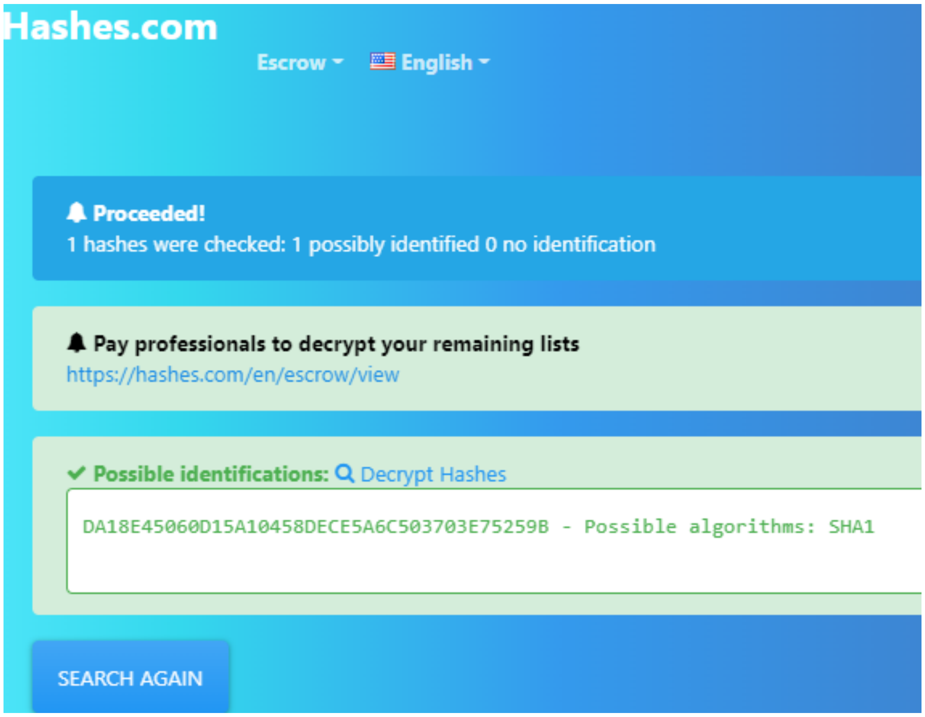
/FLAG4/

Under the [redacted] Web site, I selected DLP, then "master password hash" tab which directed me to the page below showing the users (master) hash password and /FLAG4/. I ran the hash on a hash identifier website to figure out the type and saw DA18E45060D15A10458DECE5A6C503703E75259B was a SHA1 HASH.



[redacted]/dlp/pw_hash.txt

```
This is the FLAG3 user password hash (and master):

/FLAG4/
DA18E45060D15A10458DECE5A6C503703E75259B
```



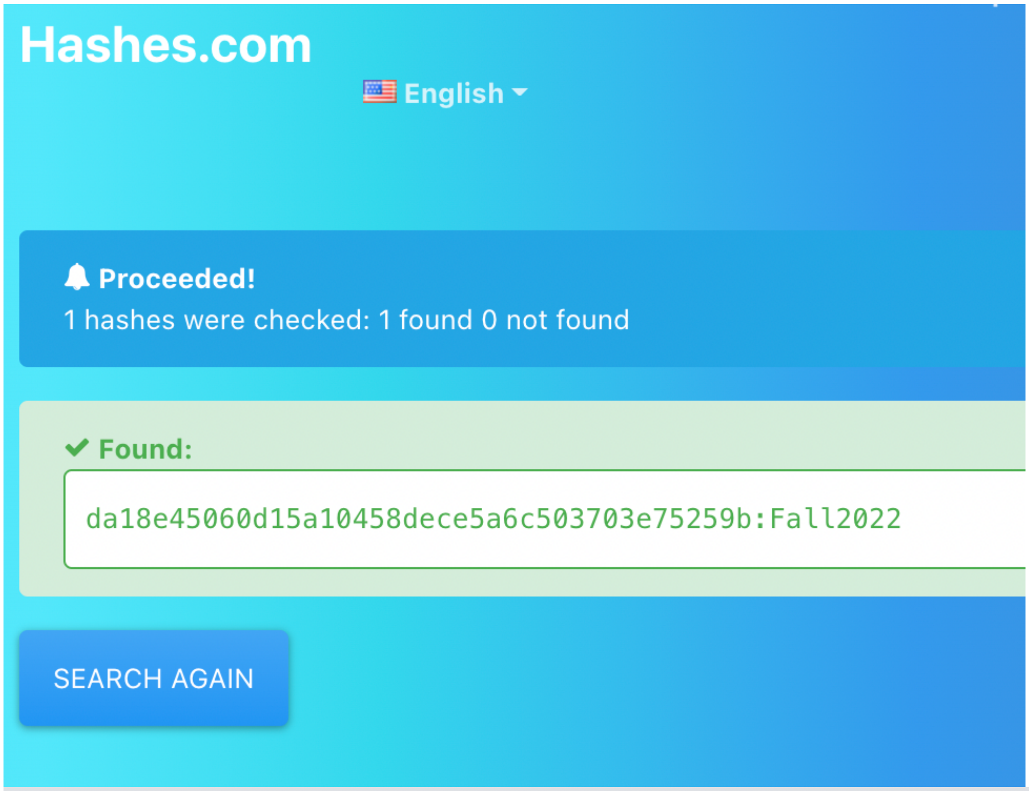
Proceeded!
1 hashes were checked: 1 possibly identified 0 no identification

Pay professionals to decrypt your remaining lists
https://hashes.com/en/escrow/view

✓ **Possible identifications:** Decrypt Hashes

```
DA18E45060D15A10458DECE5A6C503703E75259B - Possible algorithms: SHA1
```

I tried my best to crack the hash using John or Hashcat on Kali through watching videos and tutorials online but could not get it to generate. I changed the Hash from uppercase to lowercase hex and ran that through John or Hashcat, but still no results. I played around with various attack methods and type codes etc. I finally ran the hash using some online tools and found the website *hashes.com*, where I was finally able to crack the password – Fall2022. I verified it was correct through a Hash generator website by typing that password in and the SHA1 matched. I am still stumped and think it would be interesting if you could do a quick walk through on the next video chat on how to crack this hash using John or Hashcat, so I can see if was doing something wrong? Appreciate it!

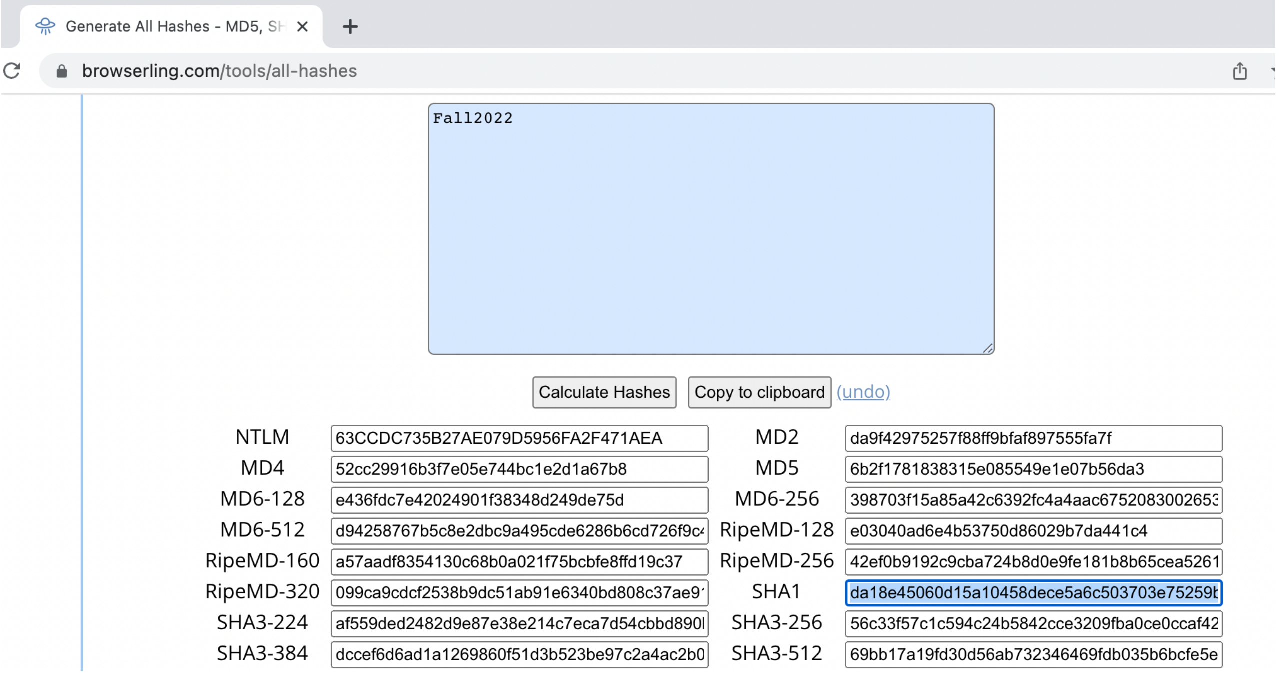


Proceeded!

1 hashes were checked: 1 found 0 not found

Found:

```
da18e45060d15a10458dece5a6c503703e75259b:Fall2022
```


Generate All Hashes - MD5, SH
browserling.com/tools/all-hashes

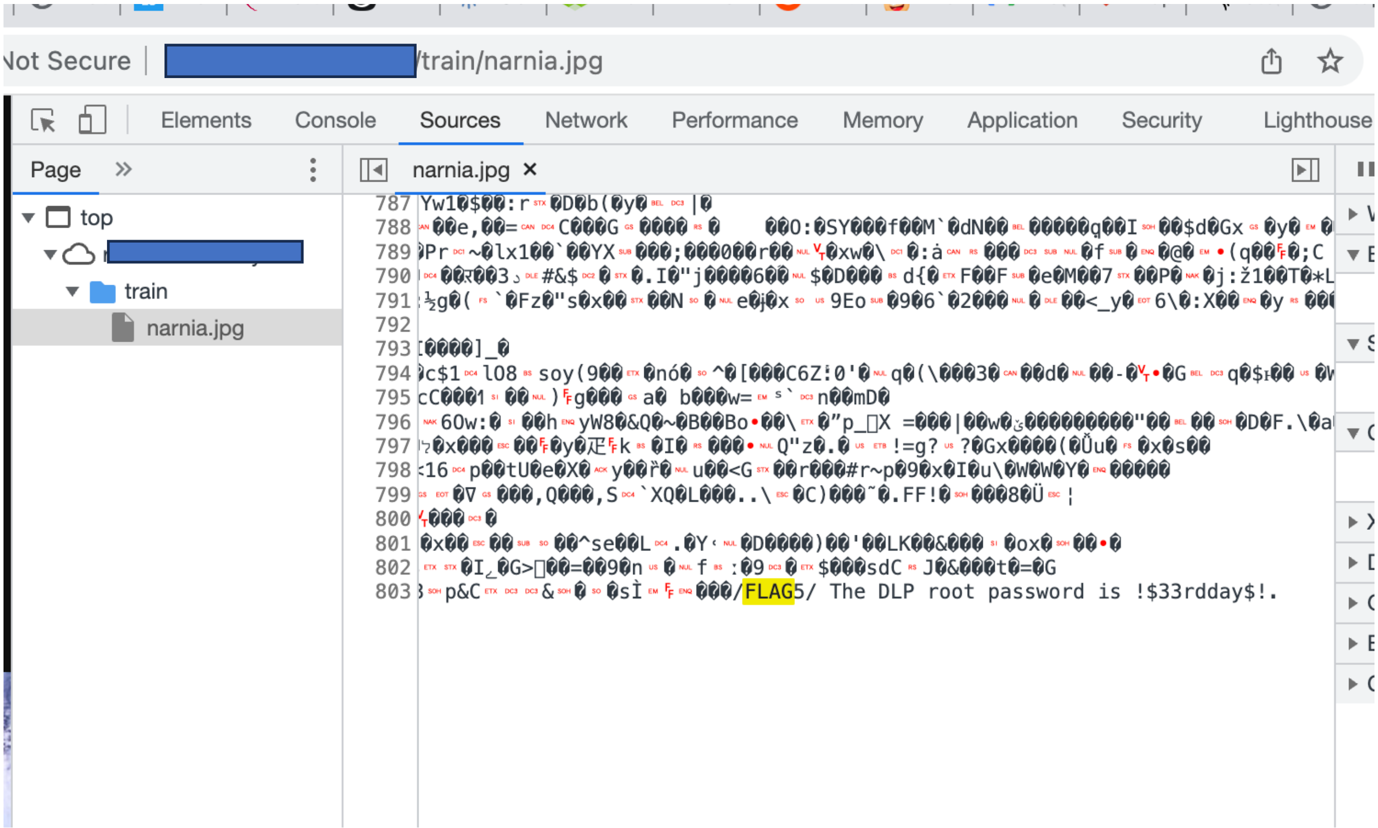
```
Fall2022
```

Calculate Hashes
Copy to clipboard
(undo)

NTLM	63CCDC735B27AE079D5956FA2F471AEA	MD2	da9f42975257f88ff9bfaf897555fa7f
MD4	52cc29916b3f7e05e744bc1e2d1a67b8	MD5	6b2f1781838315e085549e1e07b56da3
MD6-128	e436fdc7e42024901f38348d249de75d	MD6-256	398703f15a85a42c6392fc4a4aac67520830026
MD6-512	d94258767b5c8e2dbc9a495cde6286b6cd726f9c	RipeMD-128	e03040ad6e4b53750d86029b7da441c4
RipeMD-160	a57aadf8354130c68b0a021f75bcbfe8ffd19c37	RipeMD-256	42ef0b9192c9cba724b8d0e9fe181b8b65cea5261
RipeMD-320	099ca9cdcf2538b9dc51ab91e6340bd808c37ae9	SHA1	da18e45060d15a10458dece5a6c503703e75259
SHA3-224	af559ded2482d9e87e38e214c7eca7d54cbbd890	SHA3-256	56c33f57c1c594c24b5842cce3209fba0ce0ccaf42
SHA3-384	dccef6d6ad1a1269860f51d3b523be97c2a4ac2b0	SHA3-512	69bb17a19fd30d56ab732346469fdb035b6bcfe5e

/FLAG5/

On the [redacted] training page it referenced an image file “narnia.jpg’. Adding the following to the end of the URL “/train/narnia.jpg” displayed a hidden image. The source code was displayed on my browser, and I inspected the metadata within. Doing a search for “flag” found /FLAG5/ along with the DLP root password: **!$33rdday$!.**



```
Yw1�$��:r STX �D�b(�y� BEL DC3 |�
CAN ��e,��= CAN DC4 C���G GS ���� RS �     ��0:�SY���f��M`�dN�� BEL �����q��I SOH ��$d�Gx GS �y� EM �
�Pr DC1 ~�lx1��`��YX SUB ���;���0��r�� NUL VT�xw�\ DC1 �:ȧ CAN RS ��� DC3 SUB NUL �f SUB � ENQ �@� EM •(q��FF�;C
DC4 ��र��3ہ DLE #&$ DC2 � STX �.I�"j����6�� NUL $�D��� BS d{� ETX F��F SUB �e�M��7 STX ��P� NAK �j:ž1��T�∗L
½g�( FS `�Fz�"s�x�� STX ��N SO � NUL e�j�x SO US 9Eo SUB �9�6`�2��� NUL � DLE ��<_y� EOT 6\�:X�� ENQ �y RS ���

[����]_�
�c$1 DC4 l08 BS soy(9�� ETX �nó� SO ^�[���C6Z⁝0'� NUL q�(\���3� CAN ��d� NUL ��-�VT•�G BEL DC3 q�$ɪ�� US �W
cC���1 SI �� NUL )FFg��� GS a� b���w= EM s` DC3 n��mD�
NAK 60w:� SI ��h ENQ yW8�&Q�~�B��Bo•��\ ETX �”p_▯X =���|��w�ڗ���������"�� BEL �� SOH �D�F.\�a
ㄅ�x��� ESC ��FF�y�疋FFk BS �I� RS ���• NUL Q"z�.� US ETB !=g? US ?�Gx����(�Ǚu� FS �x�s��
<16 DC4 p��tU�e�X� ACK y��r̈� NUL u��<G STX ��r���#r~p�9�x�I�u\�W�W�Y� ENQ �����
GS EOT �∇ GS ���,Q���,S DC4 `XQ�L���..\ ESC �C)���˜�.FF!� SOH ���8�Ü ESC ¦
VT��� DC3 �
�x�� ESC �� SUB SO ��^se��L DC4 .�Y‹ NUL �D����)��'��LK��&��� SI �ox� SOH ��•�
ETX STX �I⸤�G>▯��=��9�n US � NUL f BS :�9 DC3 � ETX $���sdC RS J�&���t�=�G
3 SOH p&C ETX DC3 DC3 & SOH � SO �sÌ EM FF ENQ ���/FLAG5/ The DLP root password is !$33rdday$!.
```