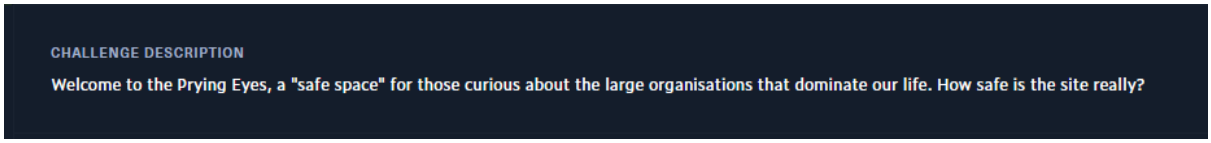
Erel Regev

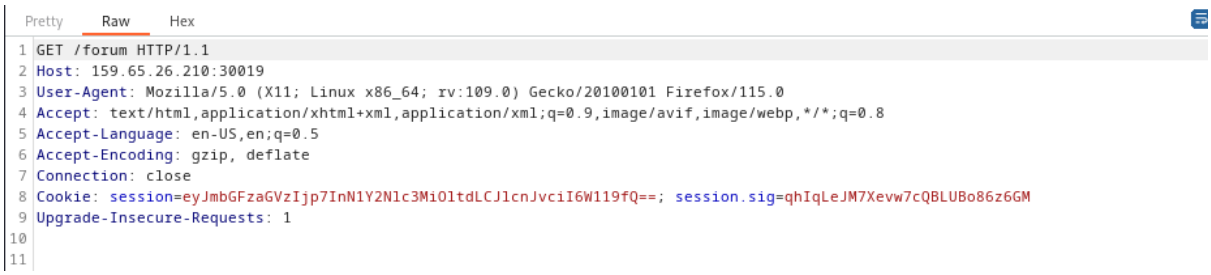
Table of Contents

Intro



Testing functionality - web

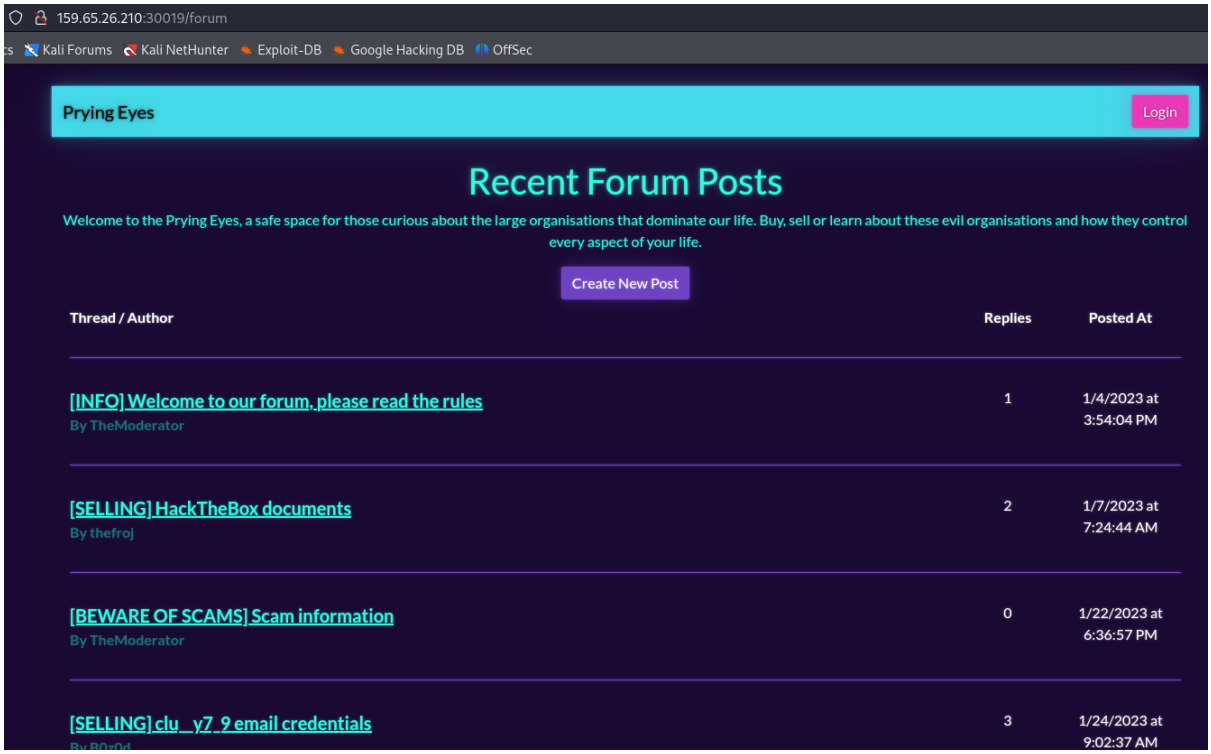
Accessing the given IP address and port:



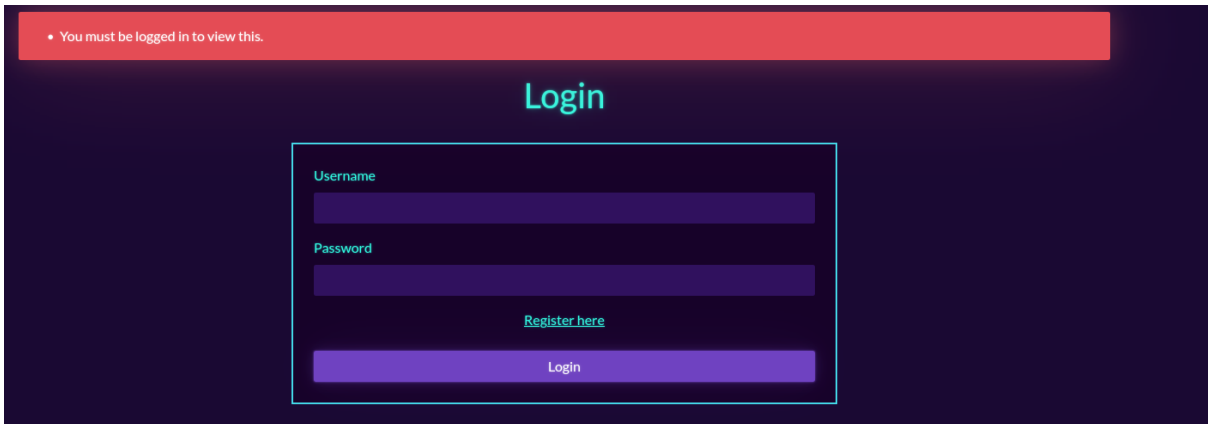
/forum

HTB Challenge: Prying Eyes - Difficulty: Medium

Erel Regev



When trying to click on one of the posts:



A login page popped up, and it seems to be possible to register.

Pretty Raw Hex

```
1  GET /auth/register HTTP/1.1
2  Host: 159.65.26.210:30019
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://159.65.26.210:30019/auth/login
9  Cookie: session=eyJmbGFzaGVzIjp7InN1Y2Nlc3MiOltdLCJlcnJvciI6W119fQ==; session.sig=qhIqLeJM7Xevw7cQBLUBo86z6GM
10 Upgrade-Insecure-Requests: 1
11
```

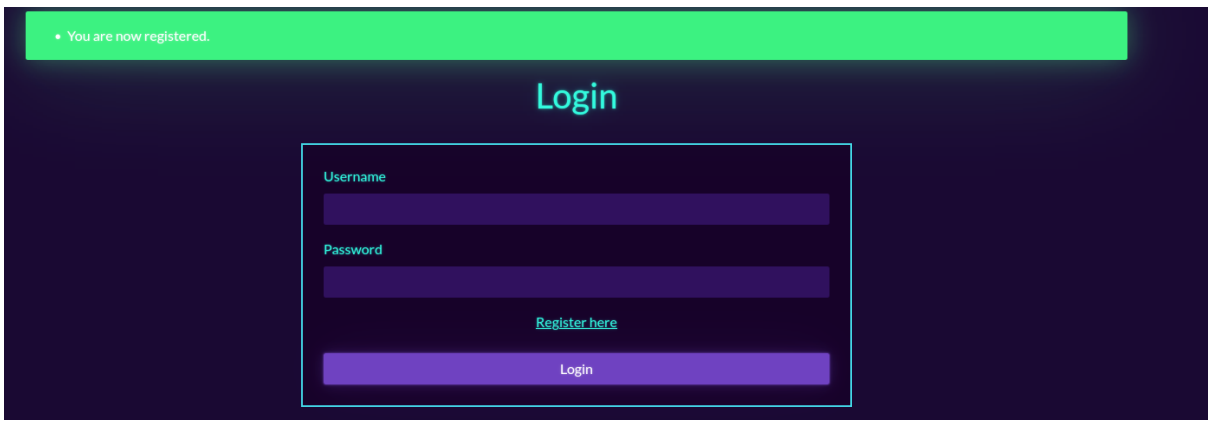
HTB Challenge: Prying Eyes - Difficulty: Medium

Erel Regev


```
Pretty  Raw  Hex
1  POST /auth/register HTTP/1.1
2  Host: 159.65.26.210:30019
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 31
9  Origin: http://159.65.26.210:30019
10 Connection: close
11 Referer: http://159.65.26.210:30019/auth/register
12 Cookie: session=eyJmbGFzaGVzIjp7InN1Y2Nlc3MiOltdLCJlcnJvciI6W119fQ==; session.sig=qhIqLeJM7Xevw7cQBLUBo86z6GM
13 Upgrade-Insecure-Requests: 1
14
15 username=Test&password=12345678
```

/auth/register

I was able to register:



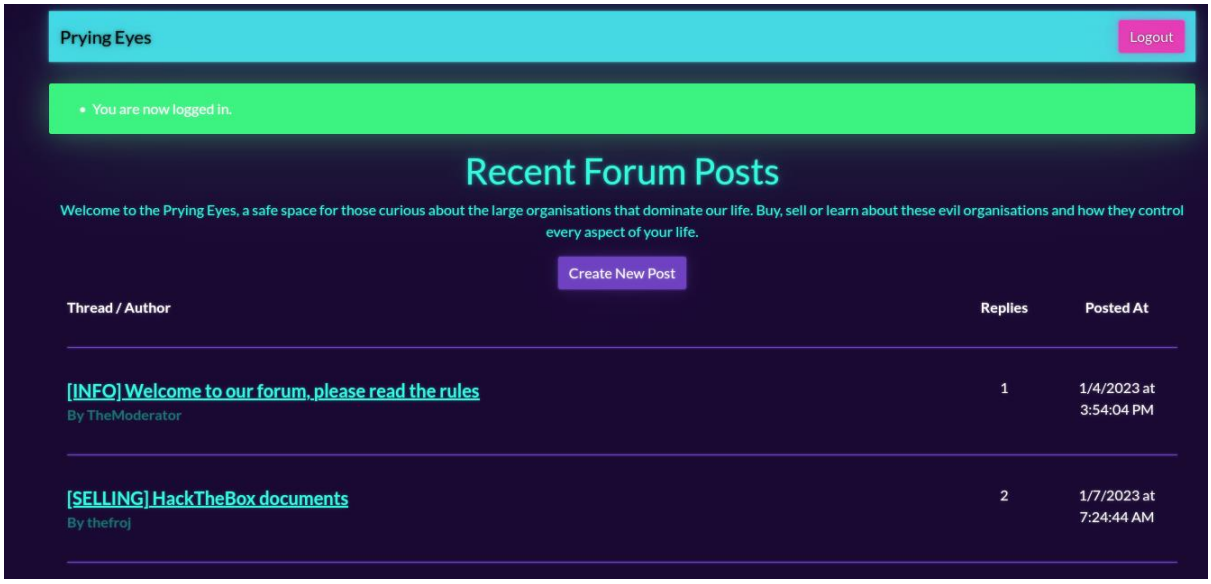
Logging in:

HTB Challenge: Prying Eyes - Difficulty: Medium

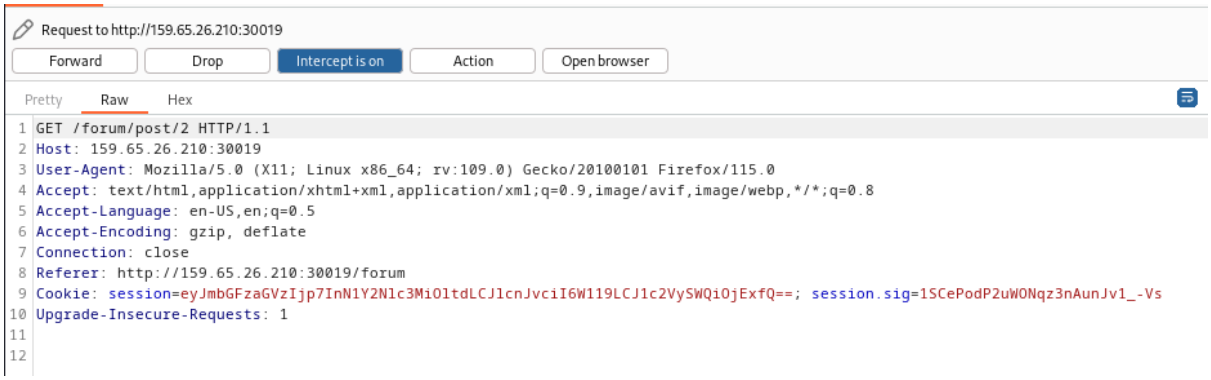
Erel Regev

```
Pretty  Raw  Hex
1  POST /auth/login HTTP/1.1
2  Host: 159.65.26.210:30019
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded
8  Content-Length: 31
9  Origin: http://159.65.26.210:30019
10 Connection: close
11 Referer: http://159.65.26.210:30019/auth/login
12 Cookie: session=eyJmbGFzaGVzIjp7InN1Y2Nlc3MiOltdLCJlcnJvciI6W119fQ==; session.sig=qhIqLeJM7Xevw7cQBLUBo86z6GM
13 Upgrade-Insecure-Requests: 1
14
15 username=Test&password=12345678
```

/auth/login



Accessing HackTheBox documents:

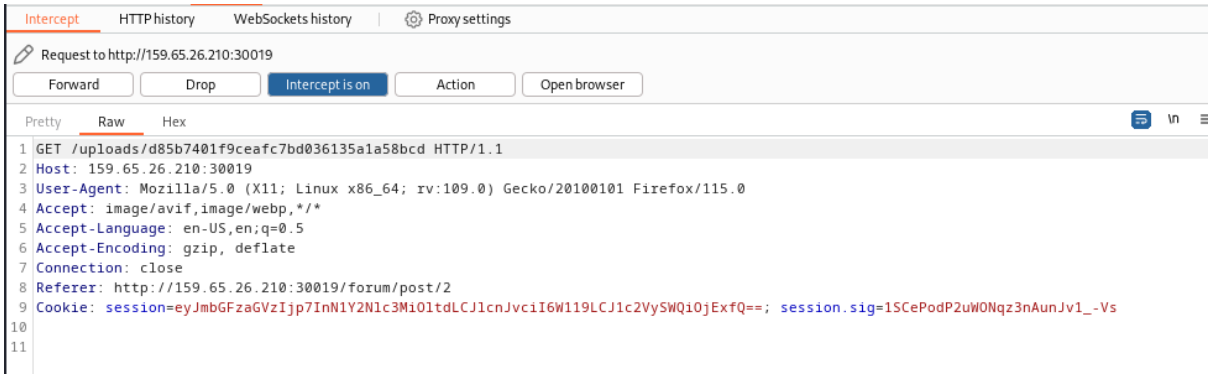


/forum/post/2

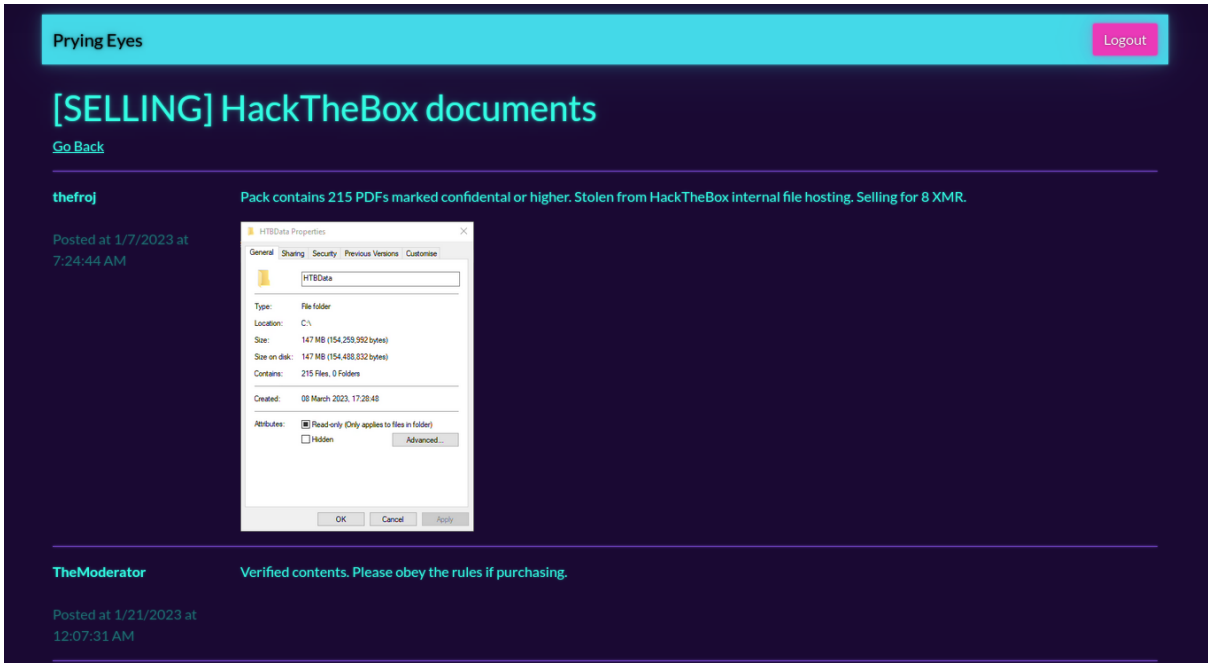
Second request:

HTB Challenge: Prying Eyes - Difficulty: Medium

Erel Regev



/uploads/d85b7401f9ceafc7bd036135a1a58bcd

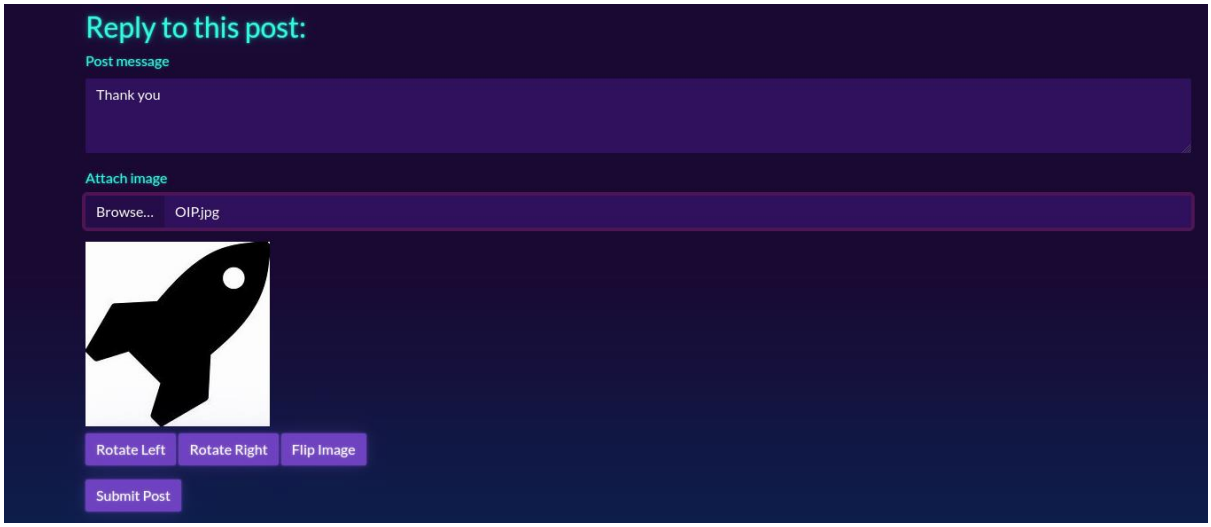


At the bottom of the page, it is possible to post a reply, which meant the server will send a POST request. As well, to upload an image.

When uploading an image (before submitting the post), it offers more functions to handle the image such as rotation and flipping.

HTB Challenge: Prying Eyes - Difficulty: Medium

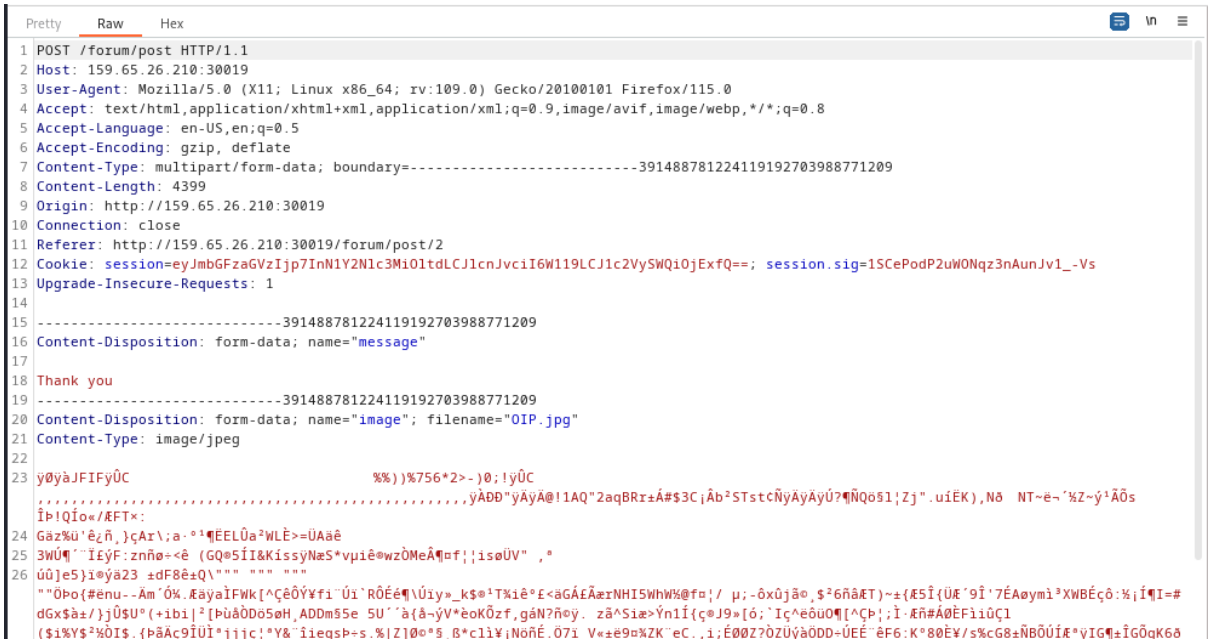
Erel Regev



Earlier when I accessed the post, it has navigated to /uploads/d85b7401f9ceafc7bd036135a1a58bcd.

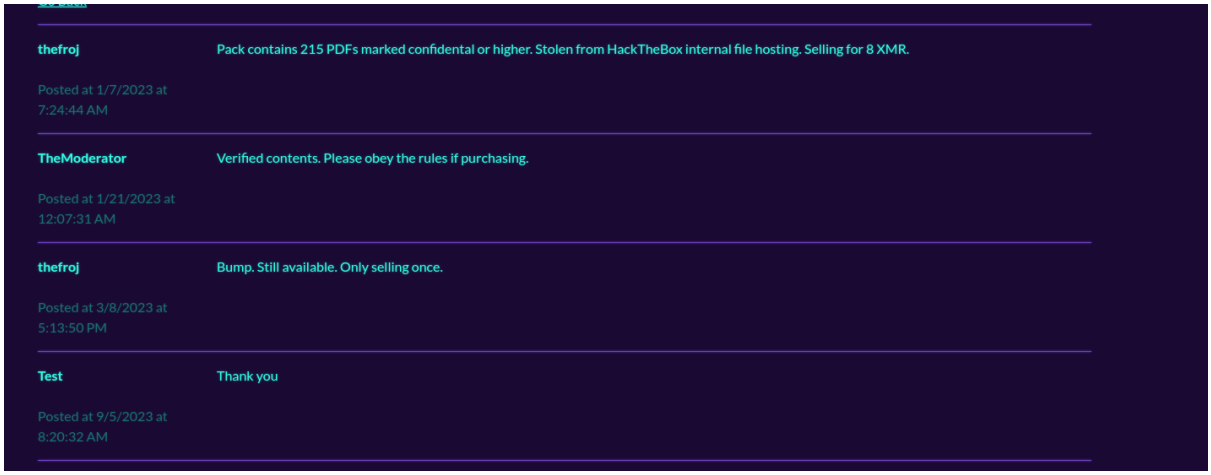
Therefore, I will probably get the path to my image as well. This feels like LFI.

Posting:



/forum/post

Erel Regev



I refreshed the page and two different requests were captured now, for the old image and the new one I uploaded.

Old:

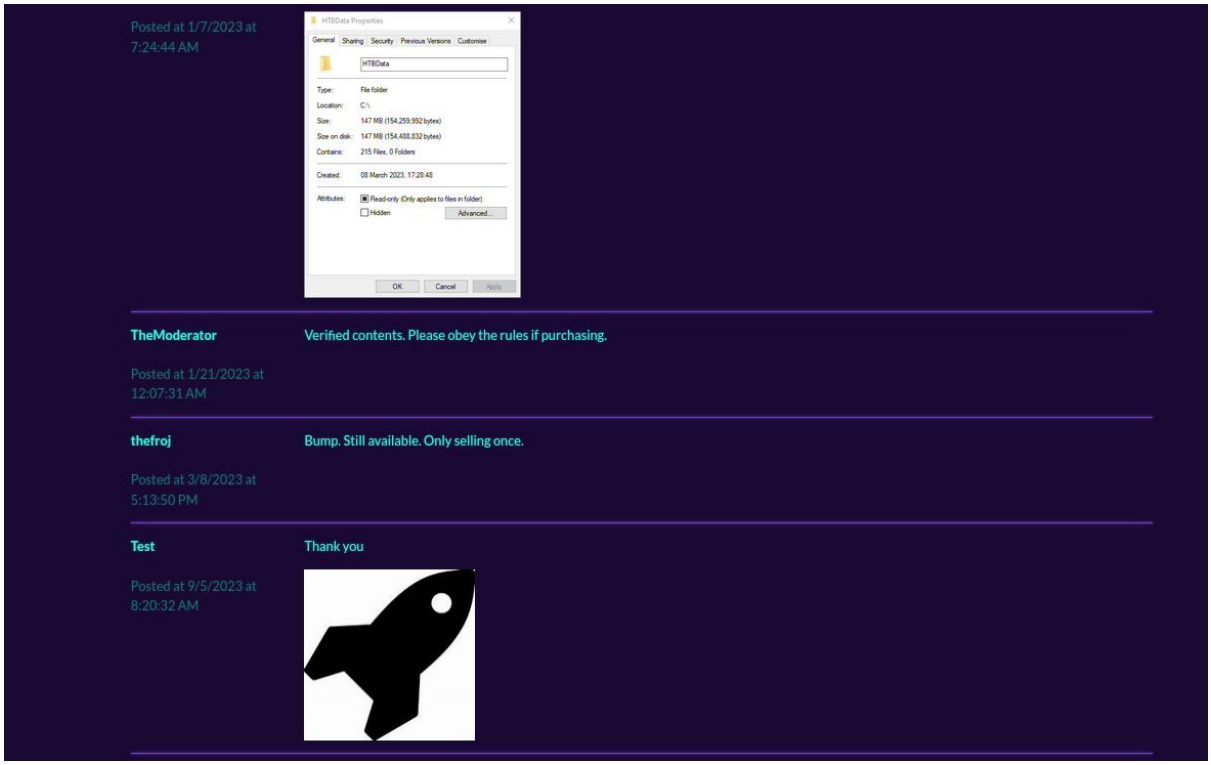
```
Pretty  Raw  Hex                                                                                                    \n
1  GET /uploads/d85b7401f9ceafc7bd036135a1a58bcd HTTP/1.1
2  Host: 159.65.26.210:30019
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: image/avif,image/webp,*/*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://159.65.26.210:30019/forum/post/2
9  Cookie: session=eyJmbGFzaGVzIjp7InN1Y2Nlc3MiOltdLCJlcnJvciI6W119LCJ1c2VySWQiOjExfQ==; session.sig=1SCePodP2uWONqz3nAunJv1_-Vs
10 If-Modified-Since: Wed, 05 Apr 2023 15:22:13 GMT
11 If-None-Match: W/"4c0f-1875202e088"
12
13
```

New:

```
Pretty  Raw  Hex                                                                                                    \n
1  GET /uploads/640dff6b6121f8e9625020cb560e9ea7 HTTP/1.1
2  Host: 159.65.26.210:30019
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4  Accept: image/avif,image/webp,*/*
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Referer: http://159.65.26.210:30019/forum/post/2
9  Cookie: session=eyJmbGFzaGVzIjp7InN1Y2Nlc3MiOltdLCJlcnJvciI6W119LCJ1c2VySWQiOjExfQ==; session.sig=1SCePodP2uWONqz3nAunJv1_-Vs
10 If-Modified-Since: Tue, 05 Sep 2023 08:20:32 GMT
11 If-None-Match: W/"1103-18a646dcc97"
12
13
```

HTB Challenge: Prying Eyes - Difficulty: Medium

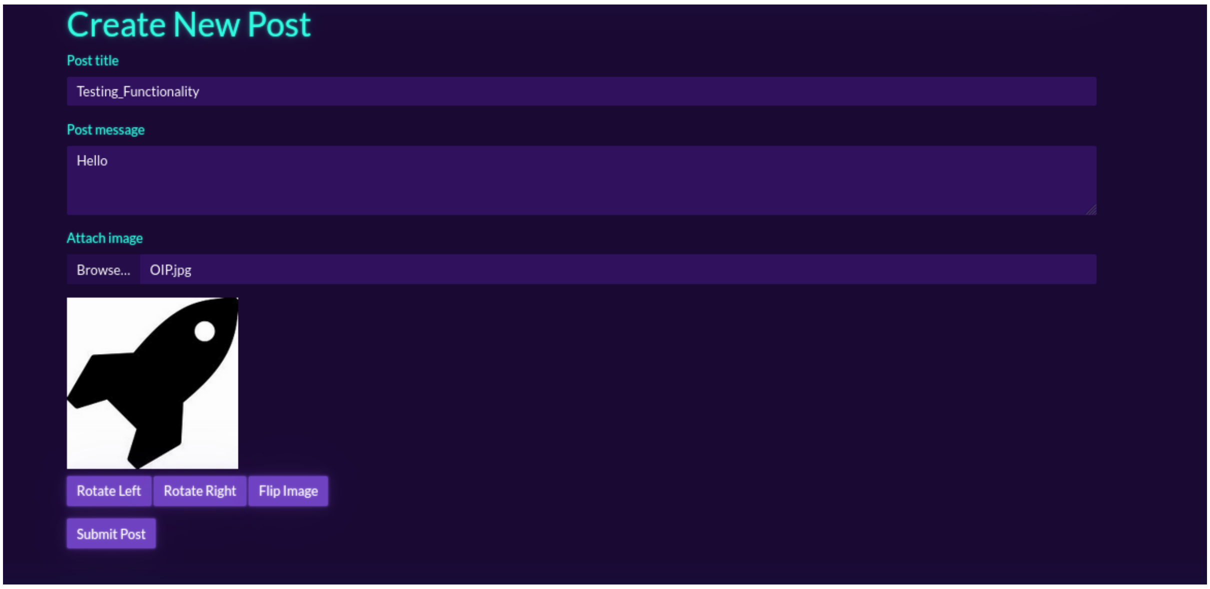
Erel Regev



It is possible to create a new post as well:

```
GET /forum/new HTTP/1.1
Host: 159.65.26.210:30019
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://159.65.26.210:30019/forum
Cookie: session=eyJmbGFzaGVzIjp7InN1Y2Nlc3MiOltdLCJlcnJvciI6W119LCJ1c2VySWQiOjExfQ==; session.sig=1SCePodP2uWONqz3nAunJv1_-Vs
Upgrade-Insecure-Requests: 1
```

/forum/new




```
POST /forum/post HTTP/1.1
Host: 159.65.26.210:30019
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------386057325629728855503413408300
Content-Length: 4412
Origin: http://159.65.26.210:30019
Connection: close
Referer: http://159.65.26.210:30019/forum/new
Cookie: session=eyJmbGFzaGVzIjp7InN1Y2N1c3MiOltdLCJ1cnJvciI6W119LCJ1c2VySWQiOjExfQ==; session.sig=1SCePodP2uWONqz3nAunJv1_-Vs
Upgrade-Insecure-Requests: 1

-----------------------------386057325629728855503413408300
Content-Disposition: form-data; name="title"

Testing_Functionality
-----------------------------386057325629728855503413408300
Content-Disposition: form-data; name="message"

Hello
-----------------------------386057325629728855503413408300
Content-Disposition: form-data; name="image"; filename="OIP.jpg"
Content-Type: image/jpeg

ÿØÿàJFIFÿÛC                              %%))%756*2>-)0;!ÿÛC
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,ÿÀÐÐ"ÿÄÿÄ@!1AQ"2aqBRr±Á#$3C¡Âb²STst¢ÑÿÄÿÄÿÚ?¶ÑQö§1¦Zj".uíËK),Nð  NT~ë¬´½Z~ý¹ÃÕs
ÎÞ!QÍo«/ÆFT×:
Gäz%ü'ê¿ñ¸}çAr\;a·°¹¶ËELÛa²WLÈ>=ÜAäê
3WÚ¶´¨Ï£ýF:znño÷<ê (GQ®5ÍI&KíssÿNæS*vµiê®wzÒMeÂ¶¤f¦¦isøÜV" ,ª
úû]e5}ï®ýä23 ±dF8ê±Q\""" """ """
""Öÿo{#ënu--Äm´Ó¼.ÆäÿaÌFWk[^ÇêÔÝ¥fi¨Úï`RÔÉé¶\Úïy»_k$®¹T%iê°£<äGÁ£ÃærNHI5WhW½@f¤¦/ µ;-ôxûjã©¸$²6ñâÆT)~±{Æ5Î{ÜÆ´9Î'7ÉAøymì³XWBÉçô:½¡Í¶I=#
dGx$à±/}jÛ$Uº(+ibi|²[ÞùåÒDö5øH¸ADDm§5e 5U´´à{å¬ýV*èoKÕzf,gáN?ñ©ÿ. zã^Siæ>Ýn1Í{ç®J9»[ó;`Iç^ëôüO¶[^ÇÞ¦;Ì·Æñ#ÁØÈFìiûÇl
($i%Y$²½ÒI$.{ÞãÄç9ÎÜÌªjjjç¦ªY&¨îieqsÞ÷s.%|Z]Ø©ª§¸ß*clì¥¡NöñÉ.Ö7ï V«±ë9¤%ZK¨eC.,i;ÉØØZ?ÒZÜýàÖDD÷ÚEÉ¨êF6:Kº8ØÈ¥/s%cG8±ÑBÕÚÍÆªÿIG¶±ÎGÕgK6ð
```

/forum/post

Pretty Raw Hex

```
GET /forum/post/17 HTTP/1.1
Host: 159.65.26.210:30019
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://159.65.26.210:30019/forum/new
Connection: close
Cookie: session=eyJmbGFzaGVzIjp7InN1Y2N1c3MiOltdLCJ1cnJvciI6W119LCJ1c2VySWQiOjExfQ==; session.sig=1SCePodP2uWONqz3nAunJv1_-Vs
Upgrade-Insecure-Requests: 1

```

/forum/post/17

HTB Challenge: Prying Eyes - Difficulty: Medium

Erel Regev

```
Pretty  Raw  Hex
1 GET /uploads/d1c7f81e0bb742991ac8e55b01c12386 HTTP/1.1
2 Host: 159.65.26.210:30019
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: image/avif,image/webp,*/*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://159.65.26.210:30019/forum/post/17
9 Cookie: session=eyJmbGFzaGVzIjp7InN1Y2Nlc3MiOltdLCJlcnJvciI6W119LCJ1c2VySWQiOjExfQ==; session.sig=1SCePodP2uWONqz3nAunJv1_-Vs
10
11
```

It feels and looks like LFI. Lets investigate the received files and see how it handles the pictures:

Since it handles images, I executed a grep command to search recursively the string “image” within the files:

```
kali@kali: ~/Desktop/Challenges/Prying_Eyes/web_prying_eyes/challenge
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~/…/Challenges/Prying_Eyes/web_prying_eyes/challenge]
└─$ grep -iRn image *
database.js:33:              attachedImage VARCHAR(256)
database.js:47:            INSERT INTO posts (createdAt, authorId, parentId, title, message, attachedImage) VALUES
database.js:127:  async createPost(authorId, parentId, title, message, image) {
database.js:131:          "INSERT INTO posts (authorId, parentId, title, message, attachedImage, createdAt) VALUES (?, ?, ?, ?, ?, ?)"
database.js:133:        resolve(await stmt.run([authorId, parentId, title, message, image, new Date().getTime()]));
index.js:39:      res.setHeader("Content-Type", "image/avif");
package.json:19:    "imagemagick-convert": "1.0.3",
package-lock.json:17:        "imagemagick-convert": "1.0.3",
package-lock.json:1036:    "node_modules/imagemagick-convert": {
package-lock.json:1038:      "resolved": "https://registry.npmjs.org/imagemagick-convert/-/imagemagick-convert-1.0.3.tgz",
package-lock.json:3131:    "imagemagick-convert": {
package-lock.json:3133:      "resolved": "https://registry.npmjs.org/imagemagick-convert/-/imagemagick-convert-1.0.3.tgz",
```

Note package-lock.json, on line 3131. Seems to be a relevant function:

```
"imagemagick-convert": {
  "version": "1.0.3",
  "resolved": "https://registry.npmjs.org/imagemagick-convert/-/imagemagick-convert-1.0.3.tgz",
  "integrity": "sha512-xkRM1qak1IiOmuNT00kQkWIISMR/MsvOYJBIiUVPBR0ucmvk1s0w44v3OL5QeObIkMA/tPCWUkrQnZD6EYBhCg=="
},
```

Imagemagick seems to be the used service:

ImageMagick, is a free and open-source software. It's like a toolbox for dealing with pictures. You can use it to show images, make new ones, change their size, alter their appearance, and even edit them. It's a versatile software for working with raster images.

I was looking for vulnerabilities for imagemagick.

Erel Regev

CVE-2022-44268

CVE-2022-44268 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

ImageMagick 7.1.0-49 is vulnerable to Information Disclosure. When it parses a PNG image (e.g., for resize), the resulting image could have embedded the content of an arbitrary. file (if the magick binary has permissions to read it).

this flaw allows an attacker to embed a specific keyword within a malicious PNG image. By specifying a particular file name in the keyword, ImageMagick inadvertently reads that file and incorporates its contents into the generated PNG image. For a detailed breakdown of this issue, you can refer to the following resource: https://www.metabaseq.com/imagemagick-zero-days/imagemagick

It's important to note that this vulnerability comes into play specifically when converting PNG files. However, it's interesting to observe from the code that the author originally intended the output image type to be AVIF.

```
59
60      try {
61        const processedImage = await convert({
62          ...convertParams,
63          srcData: req.files.image.data,
64          format: "AVIF",
65        });
66
```

Note that its in the forum.js file

One immediate consideration is the possibility of parameter overriding. This arises due to the presence of 'convertParams,' which contains parameters aside from the form. While we can pass one parameter within the form, the behavior of JavaScript is such that if a key with the same name is encountered, it will replace the previous one. Since the 'format' is passed behind 'convertParams' in the code, regardless of the format initially passed, the ultimate value will be: title, message, parentId format: "PNG" AVIF.

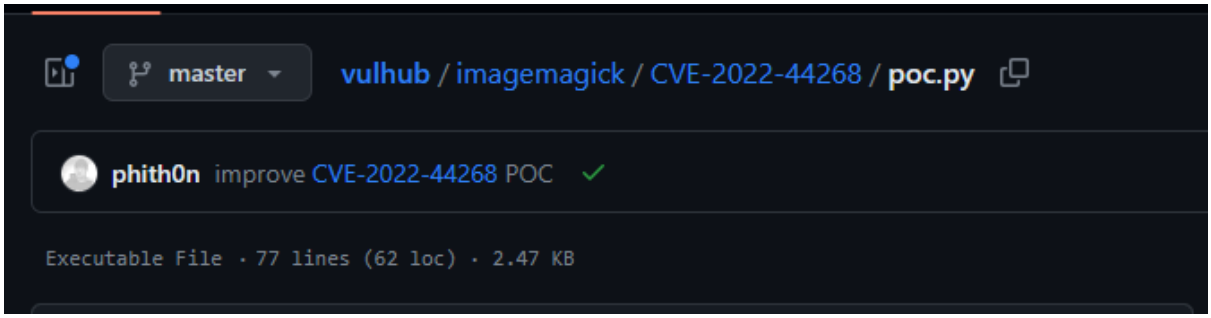
But parameters can be injected.

Given the ability to inject parameters, we're not confined by the constraints of JavaScript. Instead, we can leverage all the parameters available natively. After reviewing the ImageMagick documentation, we've identified a particular parameter that allows us to write the current image state into a file. This aligns perfectly with the requirements of CVE, as it only requires PNG when writing. By injecting this parameter, we can successfully exploit the vulnerability.

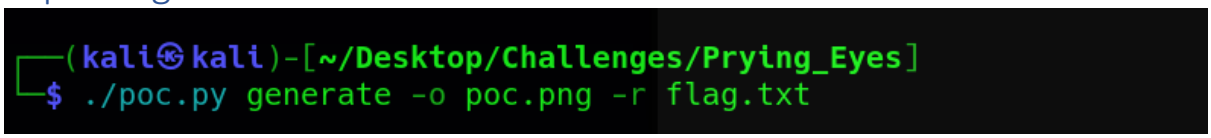
Erel Regev

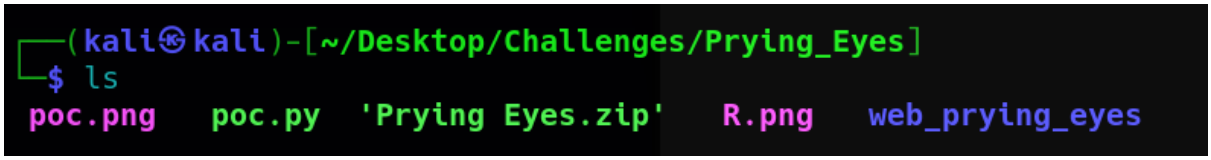
I was looking for a tool that can help exploit this vulnerability:

https://github.com/vulhub/vulhub/blob/master/imagemagick/CVE-2022-44268/poc.py



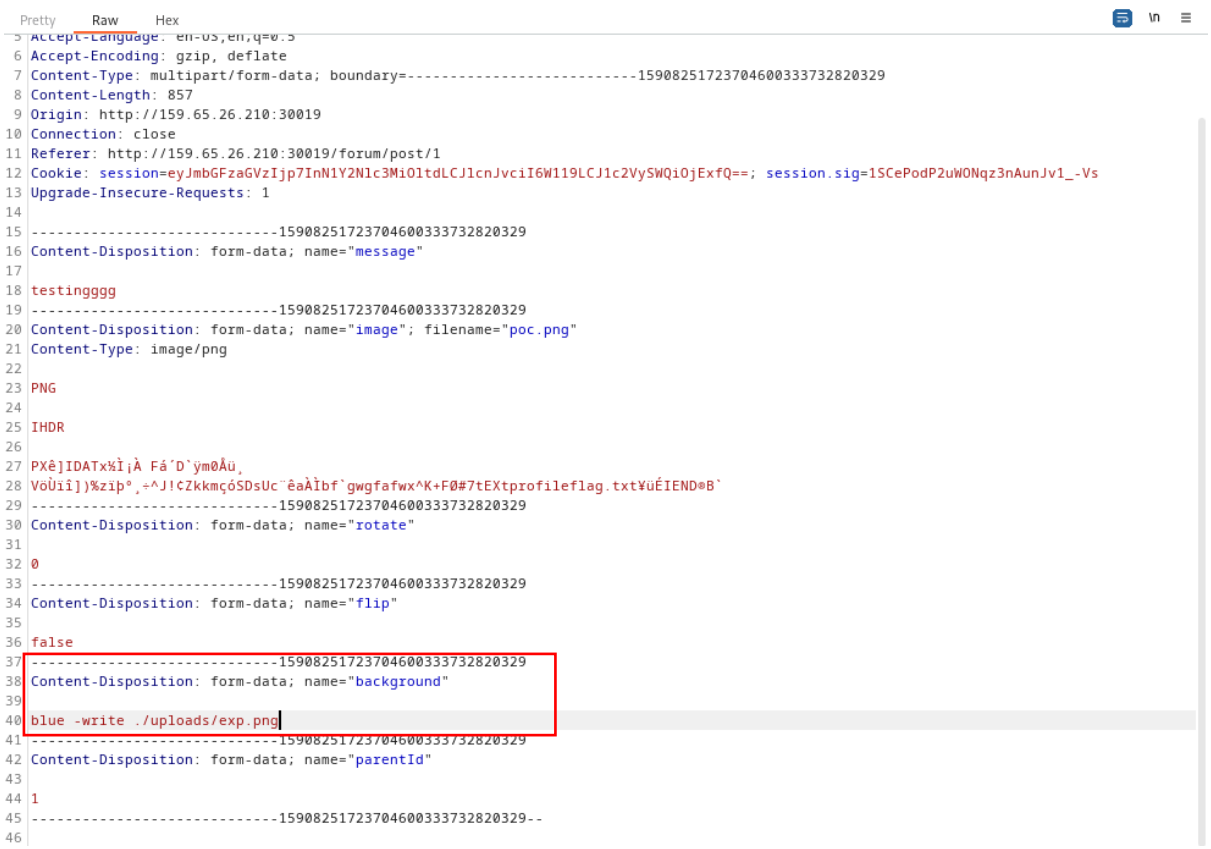
Exploiting





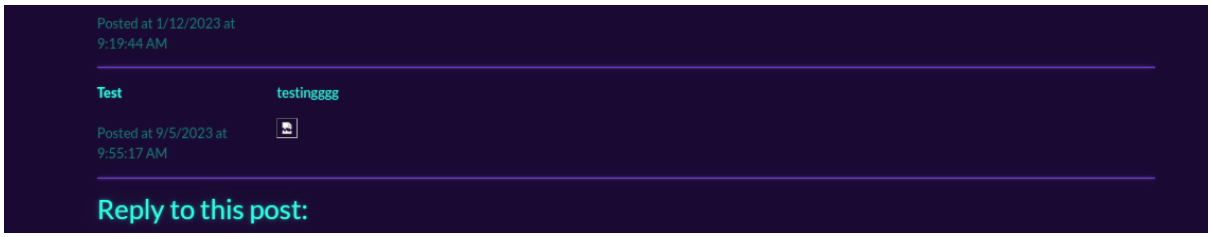
I will test it while replying to my own post from earlier:

I uploaded the malicious png file and captured the request. I added the following to the bottom of the request:

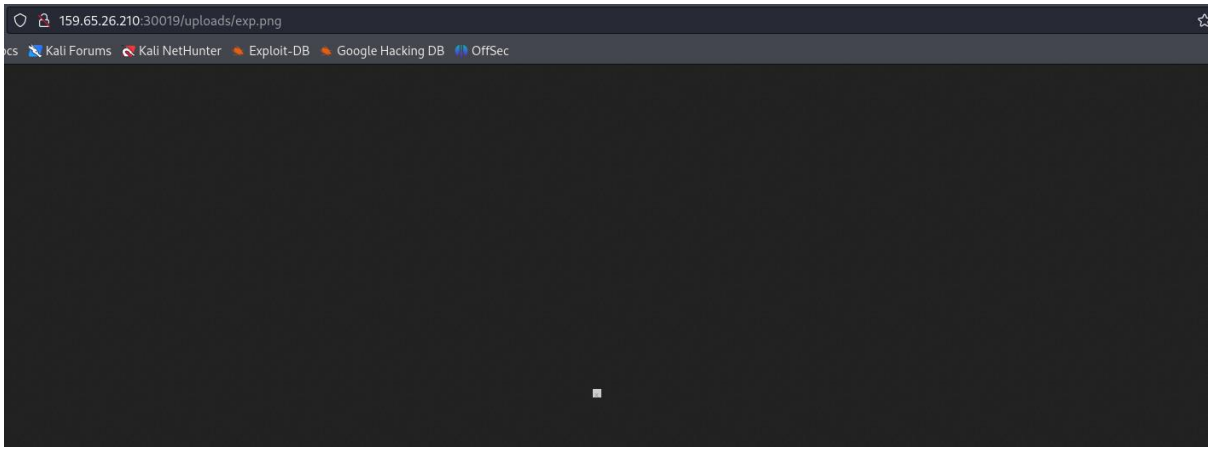


Erel Regev

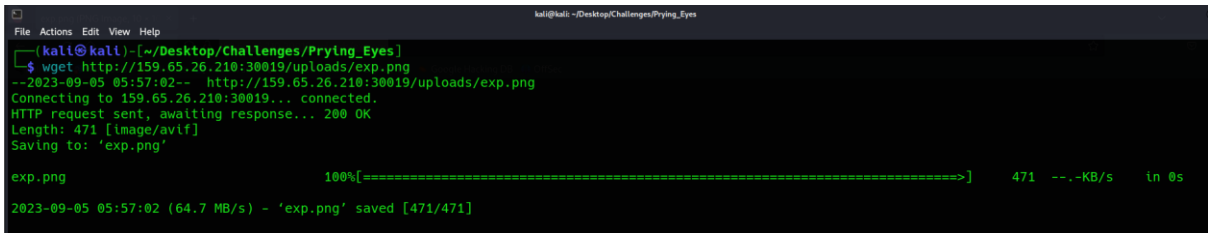
Looks like it was uploaded successfully:



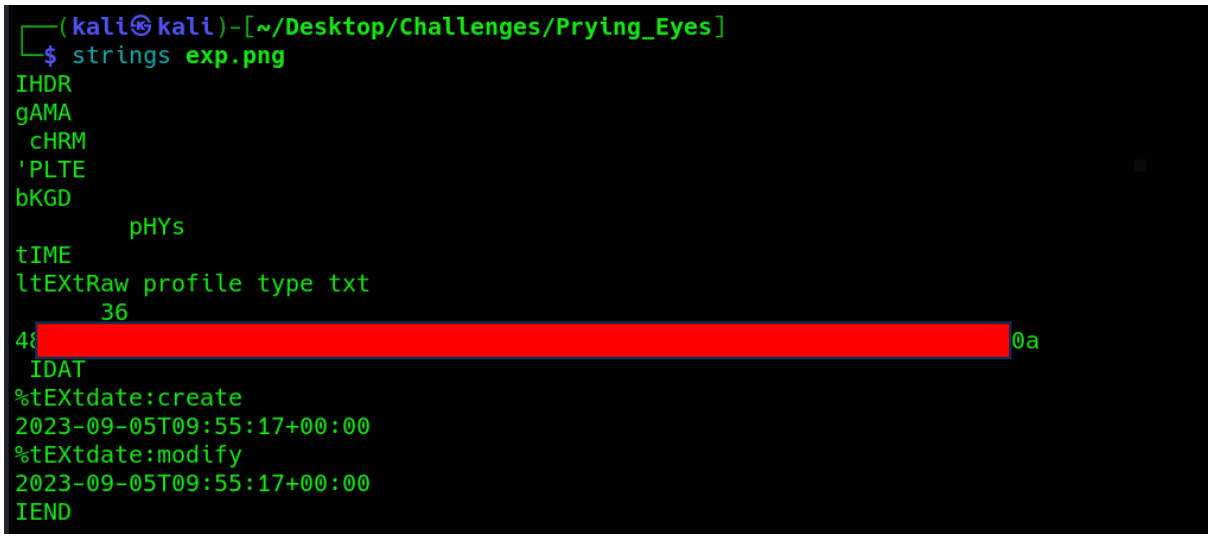
Accessing the image I wrote to /uploads/exp.png:



Downloaded the file:



I used strings on the downloaded file:



I converted the hexadecimal string using CyberChef:

HTB Challenge: Prying Eyes - Difficulty: Medium

Erel Regev