Missing Image

Category: General Skills, Web
Created: Nov 8, 2020 5:11 PM
Points: 75
Solved: Yes
Subjective Difficulty: 🔥

WriteUp:

Author: @Tibotix

🔍 Research:

The website is locatet at https://hidden.challenges.nactf.com/ .
There is an image tag that loads an image, but obviously from the wrong subdomain:

```
<!DOCTYPE html>
<html lang="en">
<head>
    <link rel="stylesheet" href="style.css">
    <title>Where's the flag?</title> <!-- (It's not here) -->
</head>
<body>
<h1>Where's the flag?</h1>
<img src="http://challenges.nactf.com/flag.png" alt="">
</body>
</html>
```

📝 Vulnerability Description:

🧠 Exploit Development:

Changing the image tag results to https://hidden.challenges.nactf.com/flag.png resulting in loading the image.

🗝 Exploit Programm:

🗯 Run Exploit:

nactf{h1dd3n_1mag3s}

FLAG: nactf{h1dd3n_1mag3s}

🗄 Summary / Difficulties:

📦 Further References:

-

🔨 Used Tools:

-

Notes:

-