File Upload Attacks

File Upload Attacks are a type of web app hack where malicious files can be uploaded to a web server and then accessed on the web app, executing the code within the uploaded malicious files

File Upload Attacks

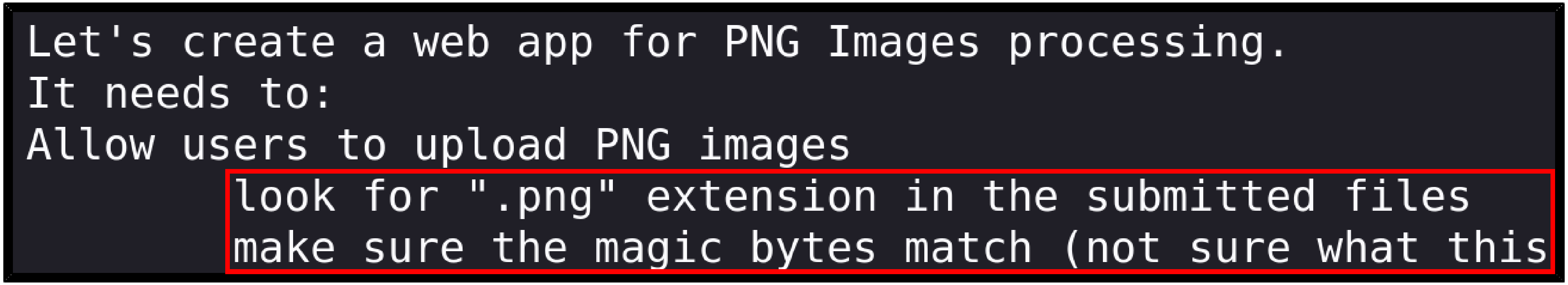
In order to perform a file upload attack, there are three conditions that must be met

1) There must be a way to upload files to a web-accessible location, via web app, or another service (e.g., FTP, SMB)

2) The upload location must be known to us

3) The app must be able to execute code: e.g., PHP or ASP

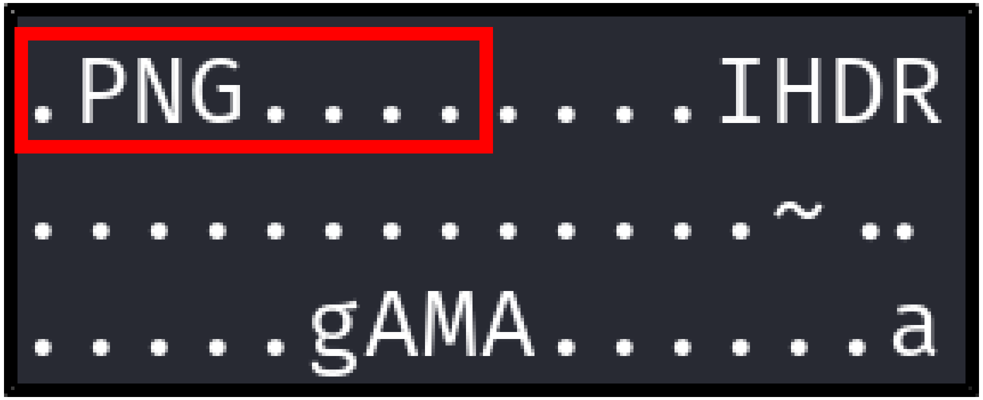
File Upload Condition



```
Let's create a web app for PNG Images processing.
It needs to:
Allow users to upload PNG images
        look for ".png" extension in the submitted files
        make sure the magic bytes match (not sure what this
```

The app lets us upload files, and a lot of apps only let you upload files of a certain type, in this case, it must have the .png file extension, and it must include the “magic bytes” for png files

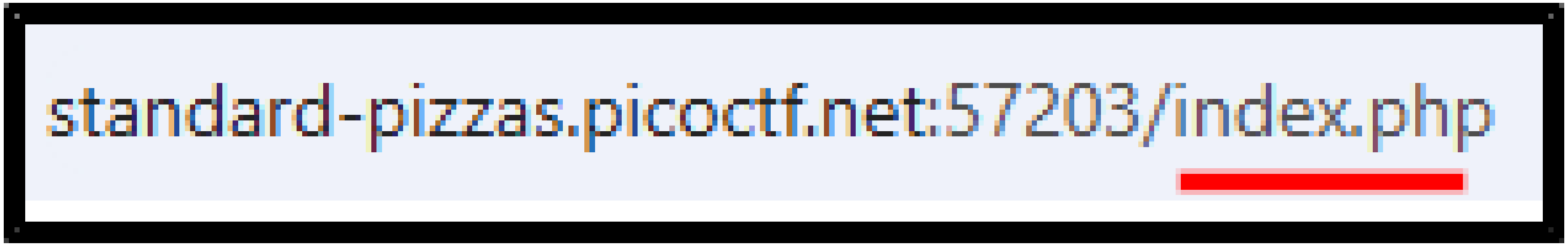
Magic Bytes



```
.PNG........IHDR
..............~..
.....gAMA......a
```

A file's magic bytes are the value of the first few bytes in a file, which identifies what type of file it is

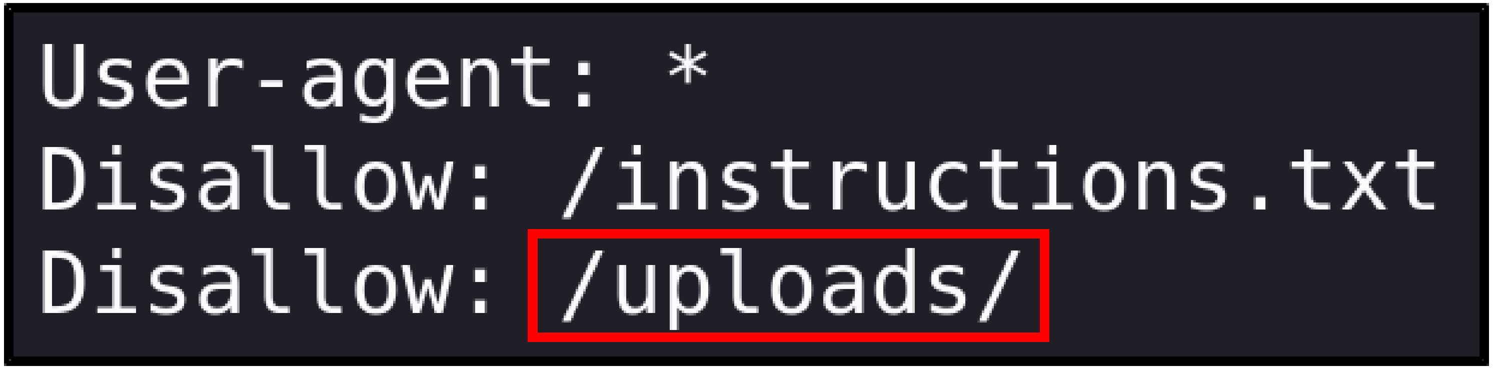
Code Execution Condition



standard-pizzas.picoctf.net:57203/index.php

File upload attacks will not work unless the web app executes code in files. PHP is a classic example, and web apps that host PHP files are a good indicator that an app is vulnerable

Known Upload Location Condition



```
User-agent: *
Disallow: /instructions.txt
Disallow: /uploads/
```

The last condition of file upload attack is the ability to access the malicious file you upload to the application. The robots.txt file in this app lets us know that there is an /uploads/ directory