n0s4n1ty - 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

n0s4n1ty - File Upload Attacks

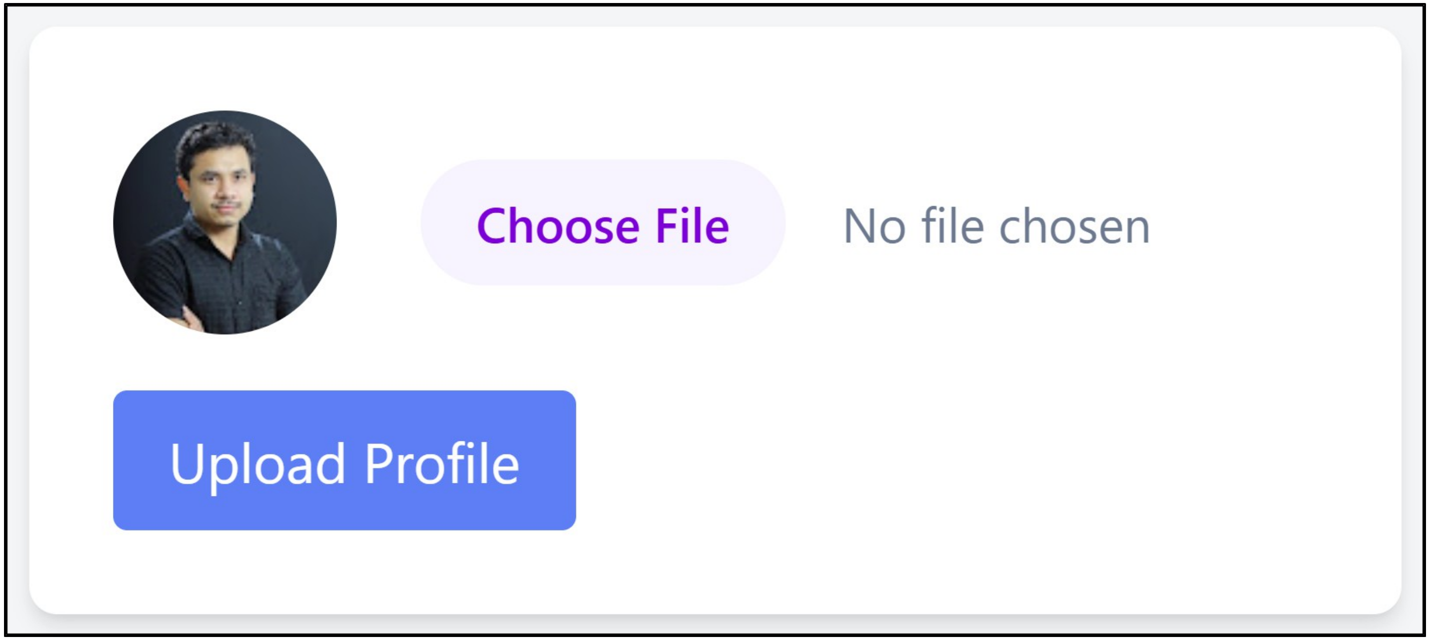
In order to perform a file upload attack, there are three conditions that must be met

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

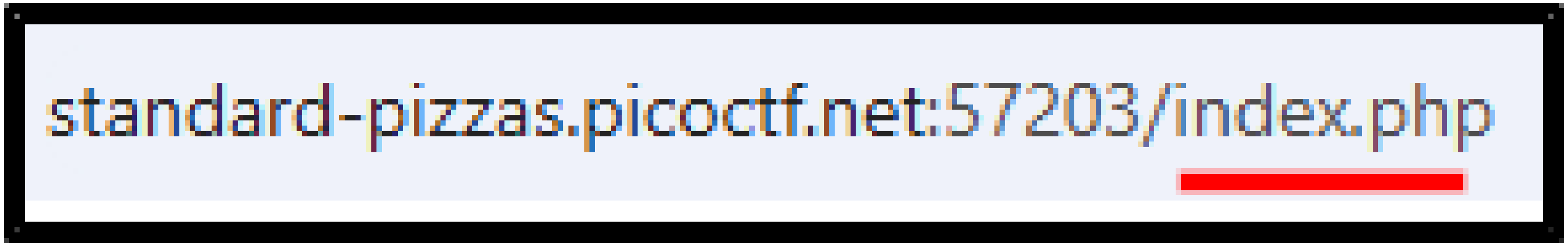
3) The app must be able to execute code: e.g., PHP or ASP

n0s4n1ty - File Upload Condition



The app lets us upload files, and a lot of apps only let you upload files of a certain type, in this case, there is no filter

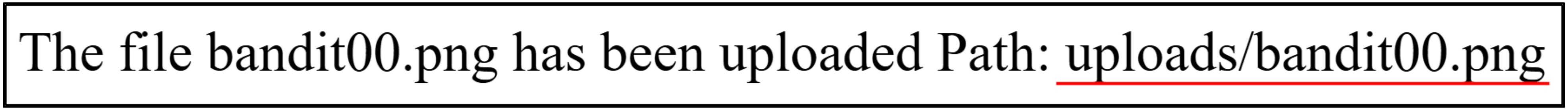
n0s4n1ty - Code Execution Condition



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

n0s4n1ty - Known Upload Location Condition



The file bandit00.png has been uploaded Path: uploads/bandit00.png

The last condition of file upload attack is the ability to access the malicious file you upload to the application. This app explicitly lets us know where uploaded files are located in the app