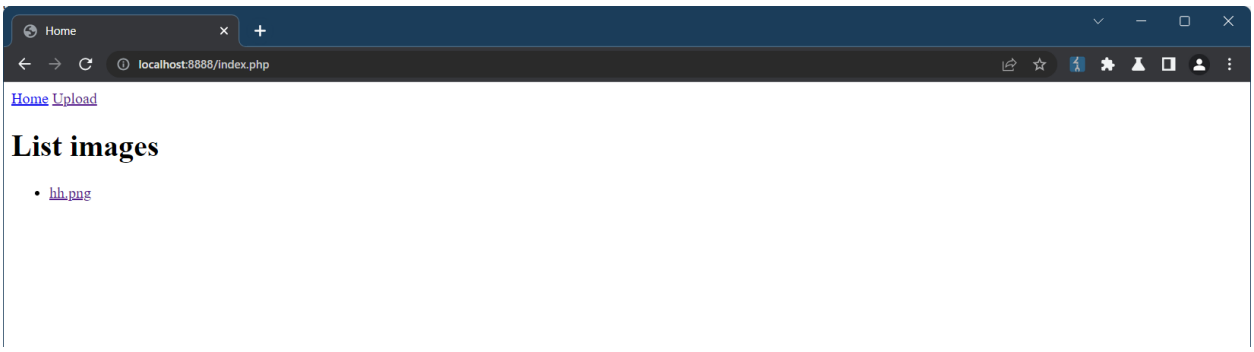
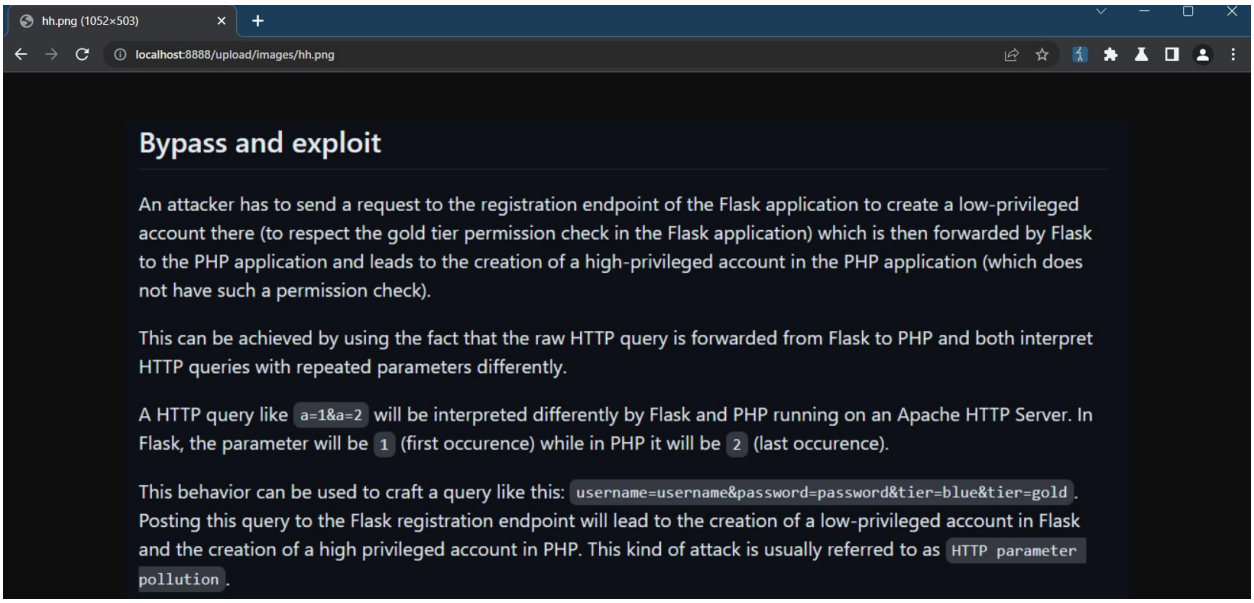
WHITE-MAGIC

I. Kiểm tra chức năng trang web

- Ở trang web này sau khi deploy xong chúng có những chức năng như sau:
  - Liệt kê các danh sách file và ảnh trong thư mục: '/upload/images/'



  - Có chức năng upload file ảnh và zip. Sau đó file zip sẽ giải nén và đưa vào '/upload/images/' để in ra danh sách file.
  - Chức năng xem file ở list images:



II. Xem source code và cách khai thác

- **Sau đây là phần xử lý chính khi mình upload file lên:**

```php
62      $whitelist_extension = ['jpg', 'jpeg', 'png', 'gif','zip'];
63      // upload file
64      $upload_dir = 'upload/';
65      $file = $_FILES['file2upload'];
66      // check empty file
67      if (empty($file['name'])){
68          echo "Error: empty file<br />";
69      }
70      $filename = basename($file['name']);
71      $ext = pathinfo($filename, PATHINFO_EXTENSION);
72      if (bodyguard($ext, $whitelist_extension)){
73          if(isImg($ext)){
74              $upload_file = $upload_dir . "images/" . basename($file['name']);
75              if (move_uploaded_file($file['tmp_name'], $upload_file)){
76                  echo "File uploaded.\n";
77              }
78          }
79          else{
80              $upload_file = $upload_dir . "zip/" . basename($file['name']);
81              if (move_uploaded_file($file['tmp_name'], $upload_file)){
82                  echo "File uploaded.\n";
83              }
84              if (unzipFile($upload_file)){
85                  getFileinPath($upload_dir . "zip/unzipped");
86              }
87              else{
88                  die("Error unzipping file.");
89                  exit();
90              }
91          }
92      }
93  echo "Back to <a href='index.php'>Home</a>";
94  ?>
```

- Chúng ta sẽ đi giải thích qua về source code để hiểu rõ hơn về chương trình:
    - Sau khi upload file lên nó sẽ đi kiểm tra extension file và đi so sánh extension có nằm trong '$whitelist_extension'. (Dòng code 72)
    - Tiếp theo nó sẽ đi kiểm tra pathinfo file. Pathinfo ở đây được hiểu là nó sẽ đây đuôi file khi mình up lên. Ví dụ file.html thì pathinfo sẽ trả về html.

```php
2 references
function isImg($extension){
    if ($extension == "jpg" || $extension == "jpeg" || $extension == "png" || $extension == "gif"){
        return true;
    }
    else{
        return false;
    }

}
```

    - Nếu là ảnh thì sẽ dc up file lên '/upload/images/file' (Dòng 75)
    - Nếu không là file ảnh nó sẽ hiểu mình đã up file zip lên.
    - Tiếp tục nó sẽ up file zip vào thư mục /upload/zip/' (Dòng 81)

- Sau đó, nó thực hiện unzip file và đưa vào thư mục ‘upload/zip/unzipped’.

```php
1 reference
function unzipFile($file){
    $zip = new ZipArchive;
    $res = $zip->open($file);
    if ($res === TRUE) {
        $zip->extractTo('upload/zip/unzipped');
        $zip->close();
        return true;
    } else {
        return false;
    }
}
```

- Tiếp tục hàm getFileinPath()

```php
1 reference
function getFileinPath($path){
    $files = array_diff(scandir($path), array('..', '.'));

    foreach ($files as $key => $value) {
        // get file extension
        $extension = pathinfo($value, PATHINFO_EXTENSION);
        if (isImg($extension)){
            if(!copyfile($path, $value)){
                die("Error: copy file failed");
                exit();
            }
        }
        // delete file
        unlink($path ."/". $value);
    }
}
```

- Nó sẽ thực hiện lấy các file trong ‘/upload/zip/unzipped’ và trả về một mảng gồm các tên file. (Dòng 44)
- Thực hiện kiểm tra pathinfo từng file. Nếu là file ảnh nó sẽ move sang ‘/upload/images/’ (Dòng 49 50)
- Tiếp tục xóa các file trong ‘/upload/zip/unzipped’ (Dòng 56)

- **Cách khai thác:**
  - Chúng ta sẽ dựa vào việc sao khi up file.zip lên nó sẽ giải nén và được đưa vào thư mục unzipped. Và nếu ta gửi nhiều request trong lúc thời gian file webshell.php mình chưa được xóa thì mình có thể đọc file và thực hiện đọc flag.
  - Source code khai thác như sau: