https://cyberjutsu.io
contact@cyberjutsu.io
+(84) 338 836 830

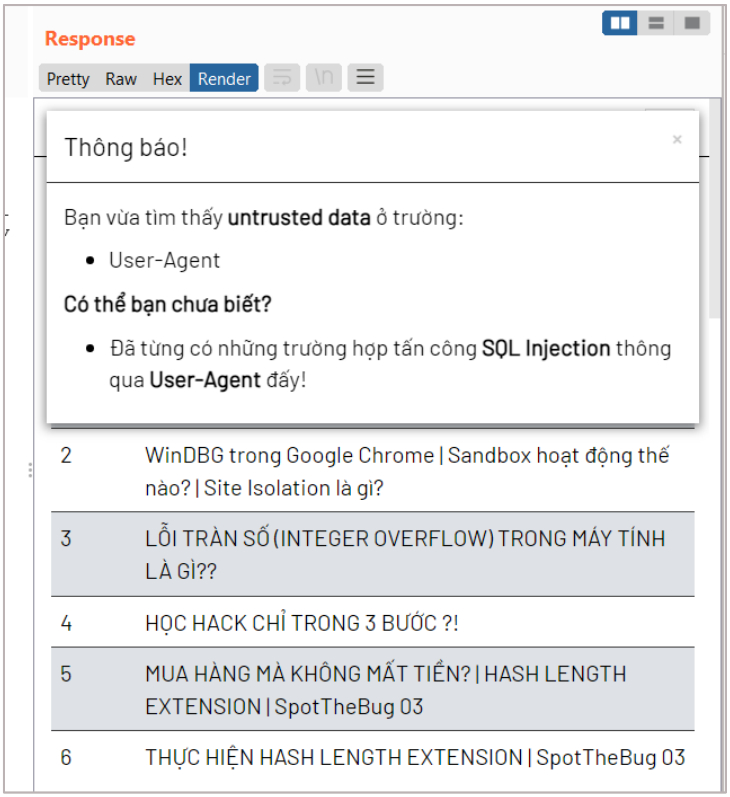
CyberJutsu

CHALLENGE WRITEUP

UNTRUSTED DATA

1. Render

Sửa bằng burp có thể xem thông báo bằng Render trong BurpSuite.



2. Solutions (20 points)

2.1. Ghi danh (2 points)

Xuất hiện ở 2 get parameter `name` và `email` tại endpoint `/register.php`

```
GET /register.php?name=test&email=test%40gmail.com HTTP/1.1
...
```

2.2. Referer (1 point)

Xuất hiện ở Header Referer

```
...
Referer: http://192.168.49.128:12000/register.php?name=test&email=test%40gmail.com
...
```

2.3. Hidden Path (1 point)

Xuất hiện tại một endpoint (path ẩn)

```
GET /test.php HTTP/1.1
...
```

2.4. Đăng kí (2 points)

Xuất hiện ở 2 post parameter `username` và `password` tại endpoint `/sign-up.php`

```
POST /sign-up.php
...
username=test&password=test
```

2.5. Đăng nhập (2 points)

Xuất hiện ở 2 post parameter `username` và `password` tại endpoint `/sign-in.php`

```
POST /sign-in.php
...
username=test&password=test
```

2.6. Training với Hokage (1 point)

Mở khi xem hết videos

```
GET /premium.php
...
```

2.7. Method ẩn (1 point)

Một trong các method sau ["OPTIONS", "TRACE", "HEAD", "PUT", "PATCH", "DELETE", "PATCH"]

```
OPTION /index.php
...
```

2.8. Profile (4 points)

Xuất hiện ở các Content-Disposition: `bio`, `filename` và các parameter: `Content-Type` của filename, File Content

```
POST /profile.php HTTP/1.1
...
------WebKitFormBoundaryZURz268sjPl6o9Q5
Content-Disposition: form-data; name="bio"

test
------WebKitFormBoundaryZURz268sjPl6o9Q5
Content-Disposition: form-data; name="file"; filename="test"
Content-Type: test

test
------WebKitFormBoundaryZURz268sjPl6o9Q5--
```

2.9. User-Agent (1 point)

Thông qua Header User-Agent.

```
GET / HTTP/1.1
...
User-Agent: test
...
```

2.10. Hidden Header (1 point)

```
GET / HTTP/1.1
...
test: test
```

2.11. Hidden Parameter (2 point)

Thêm tham số test vào gói GET nào cũng được

```
GET /?test=test HTTP/1.1
...
```

Thêm tham số test vào gói POST nào cũng được

```
POST /sign-in.php HTTP/1.1
...

username=test&password=test&test=test
```

2.12. Cookie (1 point)

Xuất hiện ở Header Cookie.

```
POST /sign-in.php HTTP/1.1
...
Cookie: PHPSESSID=39b9706993a802a0b3c523f3a6fdf8e5;test=test
...
```

2.13. Track (1 point)

Xuất hiện tại endpoint `/track.php`

```
GET /track.php?id=test HTTP/1.1
...
```