



NahamStore: Open Redirect

Introduction

Open Redirect is a vulnerability that occurs when a web application redirects the user to an external URL based on a user-controlled parameter, without properly validating the destination. It does not limit redirects to internal paths or trusted domains; the application allows an attacker to specify any URL without any validation.

Although it does not involve direct code execution or unauthorized system access, Open Redirect can be exploited by redirecting users to malicious sites that mimic the legitimate application.

Knowing this, we'll look for Open redirect errors in NahamStore.

Looking for Open Redirect

First Open Redirect

To find our first open redirect vulnerability, we'll use the **Arjun** tool. **Arjun** is an HTTP parameter enumeration tool that allows us to identify hidden parameters accepted by a web application, expanding the attack surface and making it easier to discover various types of vulnerabilities, such as **Open Redirects**. This was the result:

```
(kali㉿kali)-[~/.../THM/Machines/NahamStore/Open Redirect]
$ arjun -u http://nahamstore.thm/
[+] /[-] .[-] /(/) v2.2.7

[*] Scanning 0/1: http://nahamstore.thm/
[*] Probing the target for stability
[*] Analysing HTTP response for anomalies
[+] Extracted 1 parameter from response for testing: q
[*] Logicforcing the URL endpoint
[v] parameter detected: r, based on: http code
[v] parameter detected: q, based on: body length
[+] Parameters found: r, q
```

As we can see here, Arjun has found two parameters; the parameter **r** and the parameter **q**. To test these parameters, we simply need to place a **question mark (?)** followed by the parameter found by Arjun and ending with an **equal sign (=)**.

But first, let's choose a site to test the open redirect. We can choose any website, and if the parameter is vulnerable, we'll be automatically redirected. In this case, I'm going to set up my own HTTP server to test this vulnerability.

```
(kali㉿kali)-[~/.../THM/Machines/NahamStore/Open Redirect]
$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Now just use the parameters found to see if they redirect to our web server, starting with "/?q="

The screenshot shows a browser window with the address bar containing "http://nahamstore.thm/?q=http://...:8000". The page title is "NahamStore" and the main content says "Get The latest NahamSec Merch". A search bar at the bottom has "http://...:8000" in it.

As we can see, the parameter "q" does not redirect to our server, it only reflects what we put there in the search bar. Let's change it to "r" and see what happens:

The screenshot shows a browser window with the address bar containing "http://nahamstore.thm/?r=http://...:8000". The page title is "Directory listing for /" and the content includes a bullet point: "• You have been redirected :D".

And we have exploited the first Open Redirect. a

➡ Second Open Redirect

To find the next Open Redirect, we need to be authenticated and have a product in the basket.

The screenshot shows a browser window with the address bar containing "http://nahamstore.thm/basket". The page title is "Shopping Basket". It lists a product "Hoodie + Tee" with a cost of \$25.00. Below the basket, a "Shipping Address" section shows an error message: "Please choose an address in your address book to send to" and "You don't have any addresses in your address book!". There is a green button labeled "Add Another Address".

Once in the directory **/basket** by clicking on Add Another Address we will see something very interesting:

The screenshot shows a web browser window with the following details:

- Address Bar:** Not Secure | http://nahamstore.thm/account/addressbook?redirect_url=/basket
- Header:** NahamStore, Home, Returns, Account ▾, 0 Items
- Content:** Address Book, No Entries.
- Form:** Create Address (Title: Mr, First Name: [empty], Last Name: [empty], Address: [empty], State / County: [empty], Zip / Post Code: [empty]).

In the URL we see a parameter “**?redirect_uri=/basket**” that redirects this page back to **/basket** after filling out the form.. So, let's replace **"/basket"** with our http server address and then click on “Add Address”

The screenshot shows a web browser window with the following details:

- Address Bar:** Not Secure | [http://nahamstore.thm/account/addressbook?redirect_url=http://\[REDACTED\]:8000/](http://nahamstore.thm/account/addressbook?redirect_url=http://[REDACTED]:8000/)
- Header:** NahamStore, Home, Returns, Account ▾, 1 Item
- Content:** Address Book, No Entries.
- Form:** Create Address (Title: Mr, First Name: [empty], Last Name: [empty], Address: [empty], State / County: [empty], Zip / Post Code: [empty]).
- Buttons:** Add Address (highlighted with a red box).

This is the result:

The screenshot shows a web browser window with the following details:

- Address Bar:** Not Secure | [http://\[REDACTED\]:8000](http://[REDACTED]:8000)
- Content:** Directory listing for /
- List:** You have been redirected... Again :D

We have found our second Open Redirect.

Conclusión

These are the open redirects that can be found on NahamStore. In the next section we will be elaborating on **CSRF**.