🏪↪️ 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.

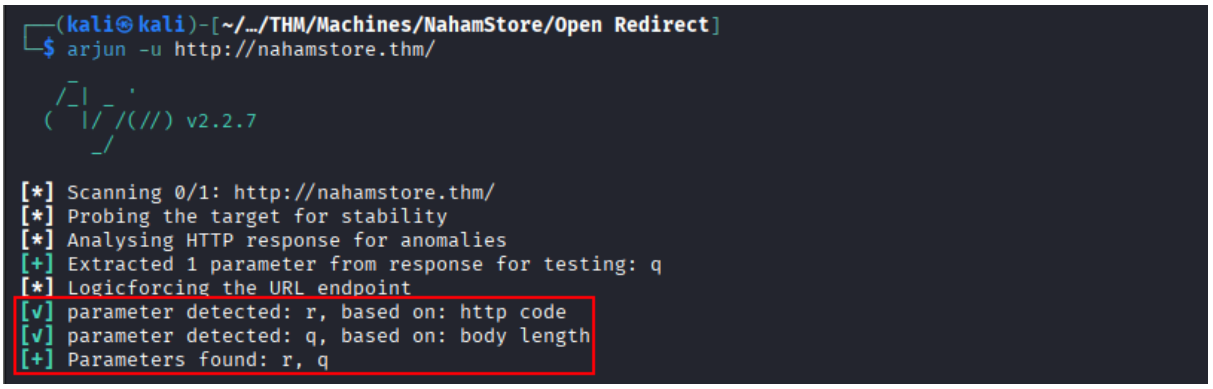
Although it does not involve direct code execution or unauthorized system access, Open Redirect can be exploited by redirecting users to malicious sites that mimic the legitimate application.

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

🕵️↪️ Looking for Open Redirect

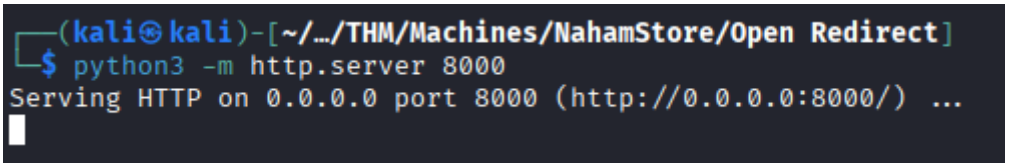
↪️ First Open Redirect

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:

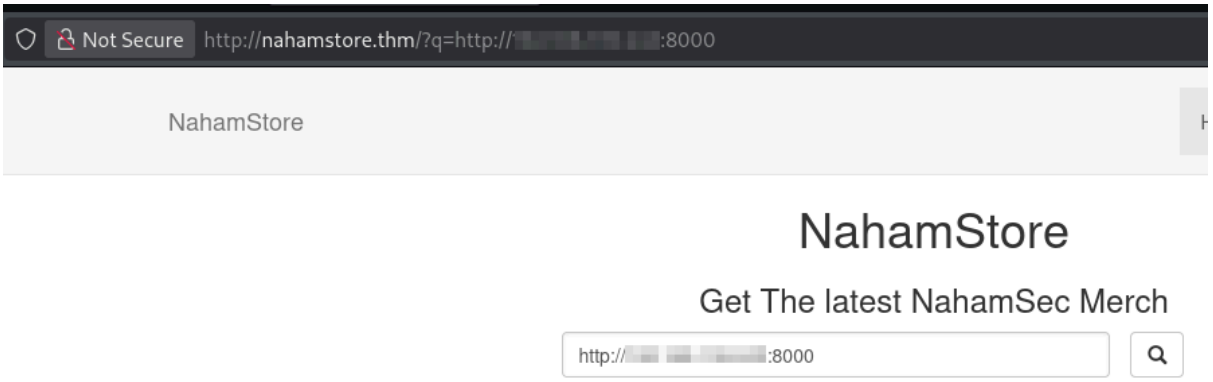


As we can see here, Arjun has found two parameters; the parameter **r** and the parameter **q**. To test these parameters, we simply need to place a **question mark (?)** followed by the parameter found by Arjun and ending with an **equal sign (=)**.

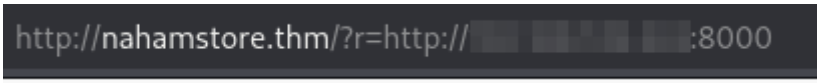
But first, let's choose a site to test the open redirect. We can choose any website, and if the parameter is vulnerable, we'll be automatically redirected. In this case, I'm going to set up my own HTTP server to test this vulnerability.

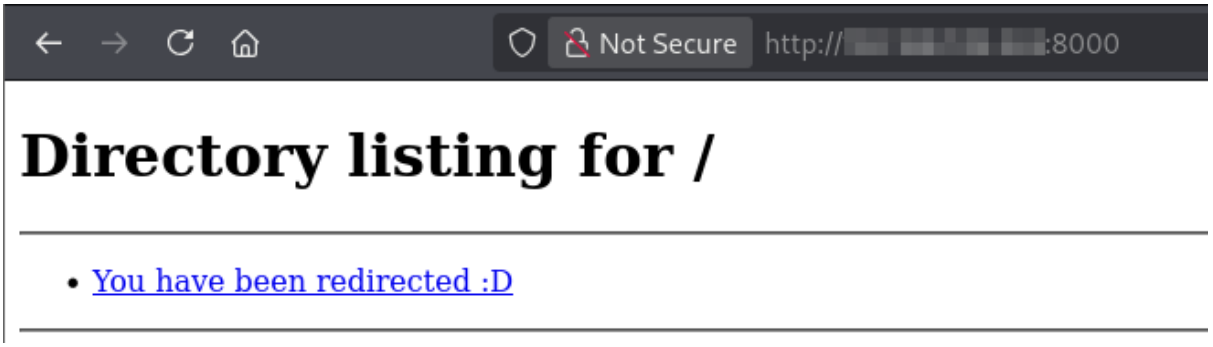


Now just use the parameters found to see if they redirect to our web server, starting with "**/?q=**"



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:

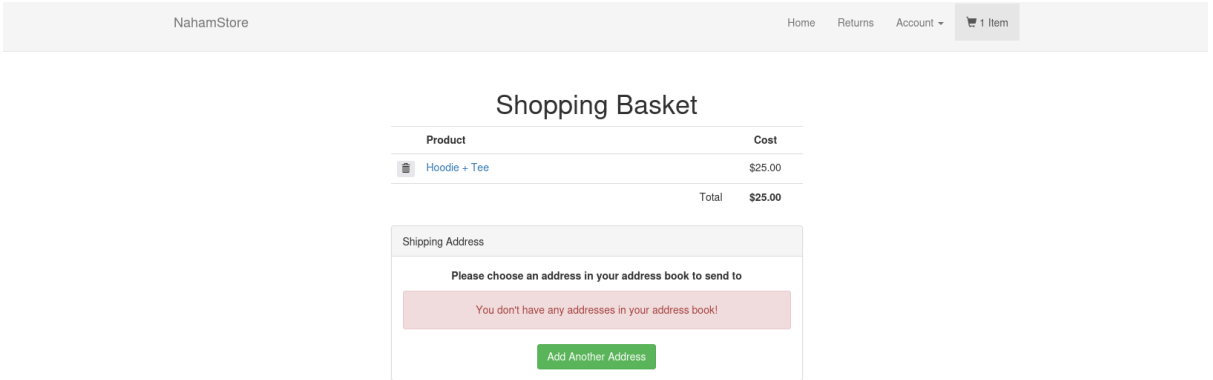




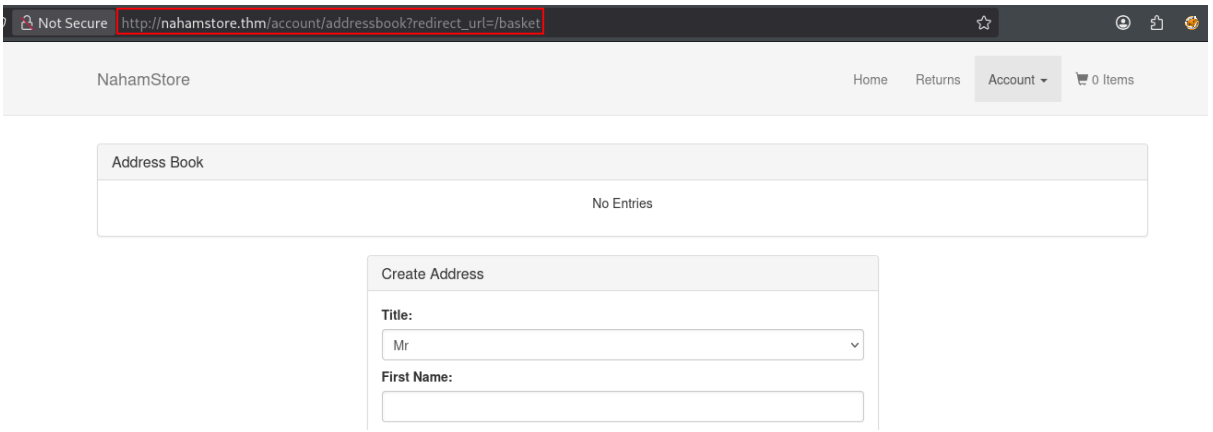
And we have exploited the first Open Redirect. a

Second Open Redirect

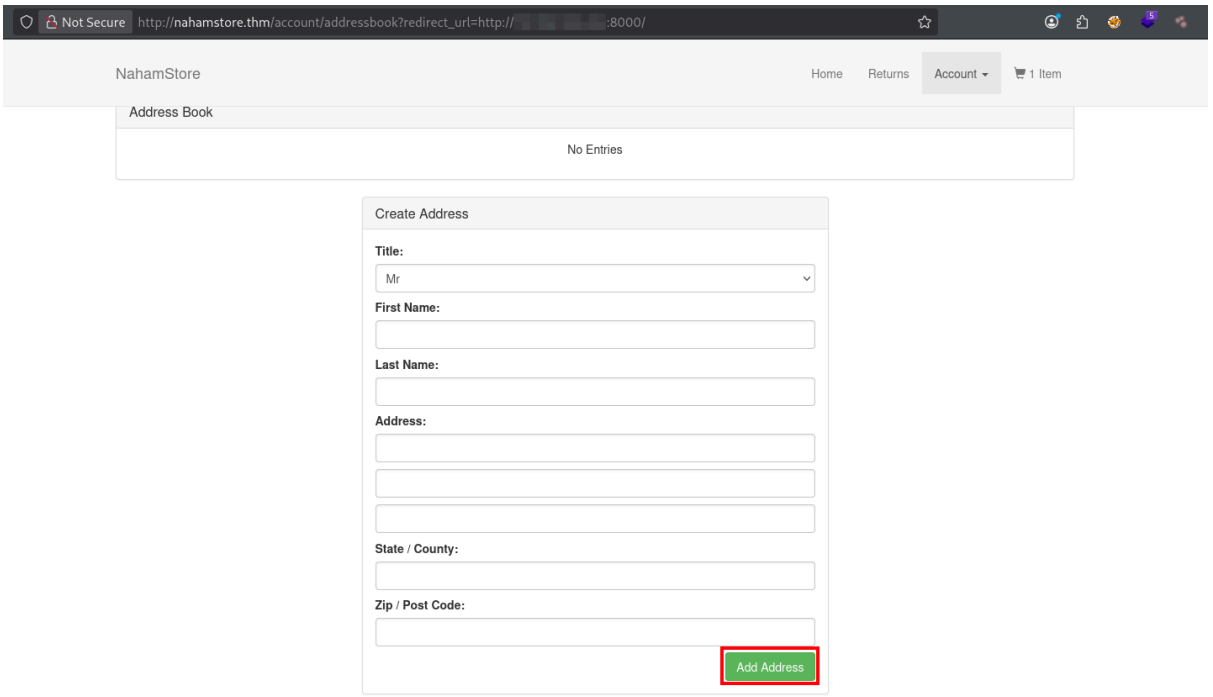
To find the next Open Redirect, we need to be authenticated and have a product in the basket.



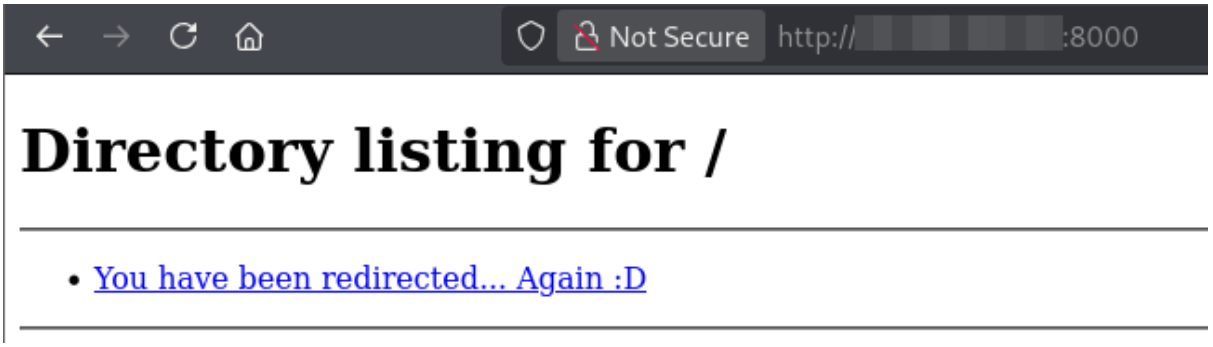
Once in the directory **/basket** by clicking on Add Another Address we will see something very interesting:



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"



This is the result:



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***.