|  |  |
| --- | --- |
| Logo  Description automatically generated | Challenge Writeup  Mystic Ensign Emporium  by Kouretas Panagiotis |

# Main Concept

# Embark on an enchanting journey through the Mystic Ensign Emporium, where each flag unfurls tales of forgotten realms and hidden lore. Let the colors sway you into a world of mystery and history, where every stitch is a spell and every emblem a charm.

# Exploitation

First of all, we deploy the challenge from CTFLib.

Then we are redirected at <http://localhost:4242/> which is the home page of the challenge as seen in Figure 2.1. It looks like a website that is selling “Mystic Ensigns”.

A screenshot of a video game

Description automatically generated

Figure 2 – Challenge’s Home Page / Mystic Ensign Shop.

When we click on one of the products we are redirected to a “flag-description” page that contains some information about the chosen flag.

A screen shot of a computer

Description automatically generated

Figure 2 - Flag description page.

With a quick look around at the page’s source code I couldn’t find something helpful for the next step of the challenge. Also, the description of the challenge looks like it does not give any practical hint.

However, if we examine the “URL” of the “flag-description” page closer, we can see that there are two parameters. One for the id of the flag page “/flag/1” and one more for the stock of the corresponding flag “in\_stock=True” as depicted in the Figure 2.3.

When we try to change the “id” of the “flag-description” page from “1” to a number up to “10” we see that we can access the descriptions of all the available flags in the store.

A screenshot of a computer

Description automatically generated

Figure 2 - Flag description page URL parameters.

So, let's experiment a little bit with the “id” parameter. I tried some numbers (>10) because 10 is the number of the currently available flags that are in stock, in case I could access any possible flag that may be unavailable and I got this response as seen in Figure 2.4.

A screen shot of a computer

Description automatically generated

Figure 2 - Flag not found error message.

Upon further investigation, I noticed through the browser developer tools there is a cookie for this website named “show\_hidden” that has the value “false”.

A screenshot of a computer

Description automatically generated

Figure 2 - Cookie value in Browser Developer tools.

I tried to manipulate this cookie, change its value and see what happens. After updating “show\_hidden” to “true” and refreshing the page this is what was displayed on the home page of the store as depicted in Figure 2.6.

A screen shot of a computer

Description automatically generated

Figure 2 - Out of stock flags appeared in the shop.

Two new flags that are out of stock appeared in the shop. If we click on each one of them, we get the response that “This flag is not in stock” on the “flag-description” page as seen in the Figure 2.7.

A screen shot of a computer

Description automatically generated

Figure 2 - Flag not in stock error message.

What if we try to manipulate the second parameter now?

Changing the stock parameter from “in\_stock=False” to “in\_stock=True”, we are getting back the description of the flag that was out of stock and not available for sale to the customers.

A screenshot of a computer

Description automatically generated

Figure 2 - Manipulating "in\_stock" parameter.

Then we notice that this flag’s page id is “/flag/100”. Now let's try to see what the other unavailable flag displays on the description page if we update its stock parameter.

A close up of a screen

Description automatically generated

Figure 2 - Hidden flag successfully retrieved.

BANG, we found the hidden FLAG in the “Mystic Ensign Emporium”.

CTFLIB{Acc3ss\_C0ntr0l\_V4ln\_Expl01t3d}