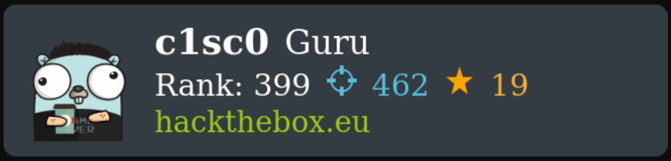
Hack The Box - Writeup

Forge

c1sc0



c1sc0 Guru
Rank: 399 ⌖ 462 ★ 19
hackthebox.eu

September 22, 2021

Table of Content

Overview

IP	Difficulty
10.10.11.111	Medium

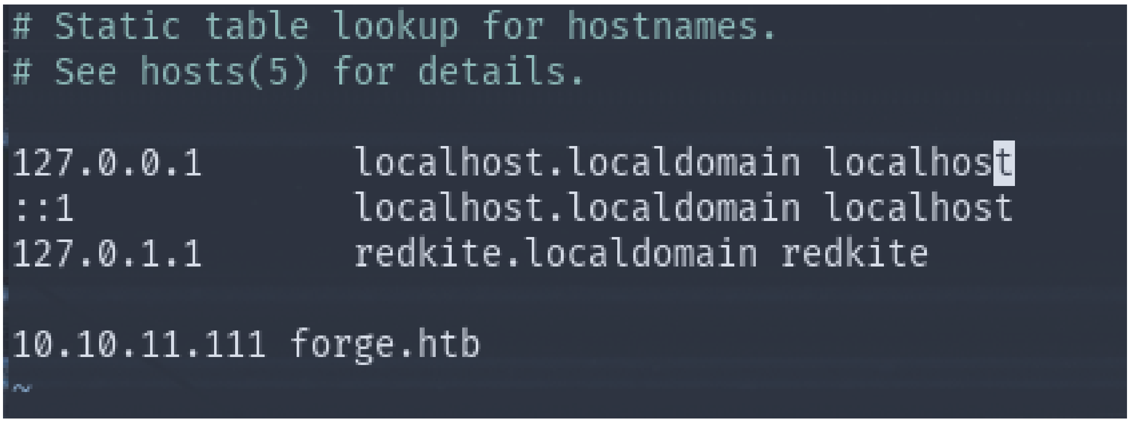
Nmap

`sudo nmap -sC -sV -oA nmap/forge -vvv 10.10.11.111`

```
PORT   STATE    SERVICE REASON         VERSION
21/tcp filtered ftp     no-response
22/tcp open     ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4f:78:65:66:29:e4:87:6b:3c:cc:b4:3a:d2:57:20:ac (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQA...
|   256 79:df:3a:f1:fe:87:4a:57:b0:fd:4e:d0:54:c6:28:d9 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTI...
|   256 b0:58:11:40:6d:8c:bd:c5:72:aa:83:08:c5:51:fb:33 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5A...
80/tcp open     http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Did not follow redirect to http://forge.htb
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

/etc/hosts

80 redirects to `forge.htb`. So adding it to `/etc/hosts`



```
# Static table lookup for hostnames.
# See hosts(5) for details.

127.0.0.1       localhost.localdomain localhost
::1             localhost.localdomain localhost
127.0.1.1       redkite.localdomain redkite

10.10.11.111 forge.htb
~
```

Figure 1: added forge.htb to /etc/hosts

Website

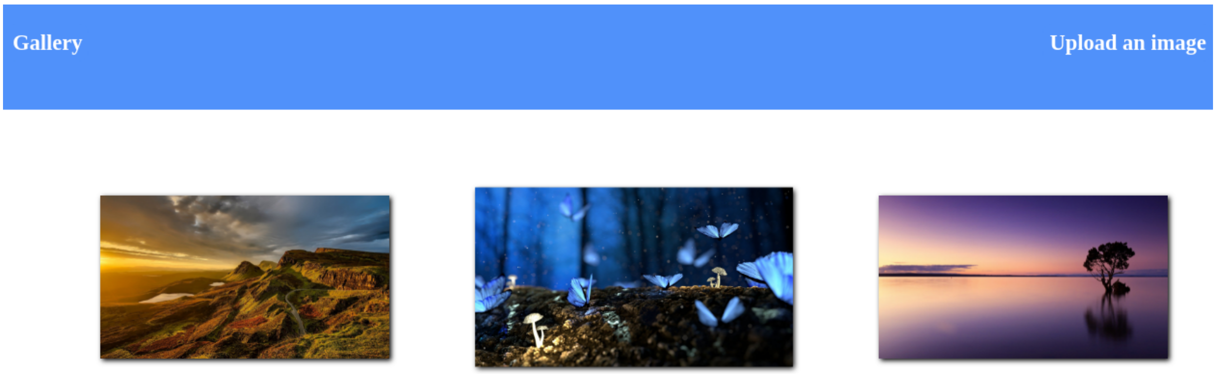


Figure 2: Website on port 80 for forge.htb

Interesting “Upload an image” button top right

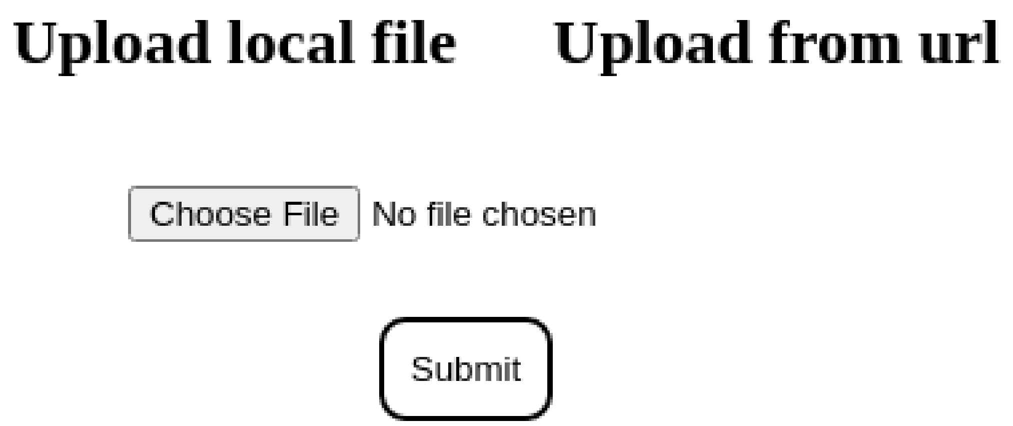


Figure 3: Upload image page

Looks like you can either provide file or enter URL.

Uploading images works, whereas uploading a cmd shell for example doesn't.

If you try and choose to upload from URL the box will callback to you:

```
> sudo ncat -lnvp 80
[sudo] password for patrick:
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.10.11.111.
Ncat: Connection from 10.10.11.111:38550.
GET /foo.png HTTP/1.1
Host: 10.10.14.8
User-Agent: python-requests/2.25.1
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

Subdomain enumeration

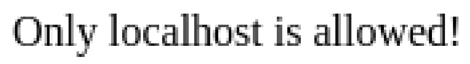
Wfuzz will reveal another subdomain:

```
> wfuzz -c -w ~/tools/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt -u 'http://forge.htb' -H "Host: FUZZ.forge.htb" --hw 26
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************
```

```

Target: http://forge.htb/
Total requests: 4989

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000024:   200        1 L      4 W        27 Ch       "admin"

Total time: 0
Processed Requests: 4989
Filtered Requests: 4988
Requests/sec.: 0
```

So adding it to /etc/hosts and again look at the resulting page.

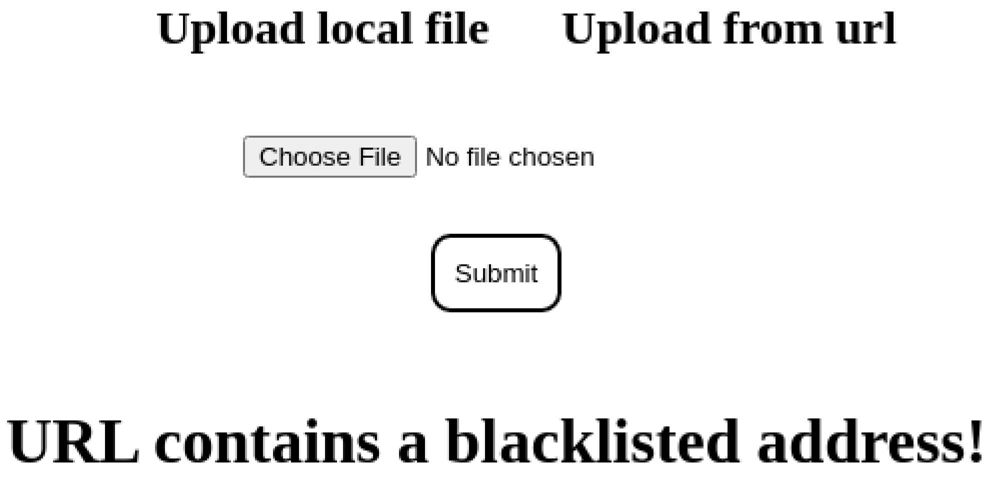
admin.forge.htb



Only localhost is allowed!

Figure 4: Only localhost is allowed

So the idea is to leverage a vulnerablity at the upload from URL part to look at `admin.forge.htb` from within the internal network.



URL contains a blacklisted address!

Figure 5: Blacklist is in place

It looks like it is blacklisted though