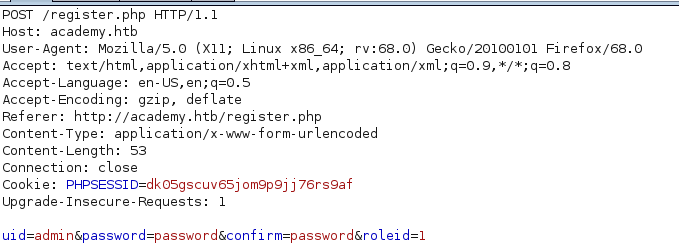
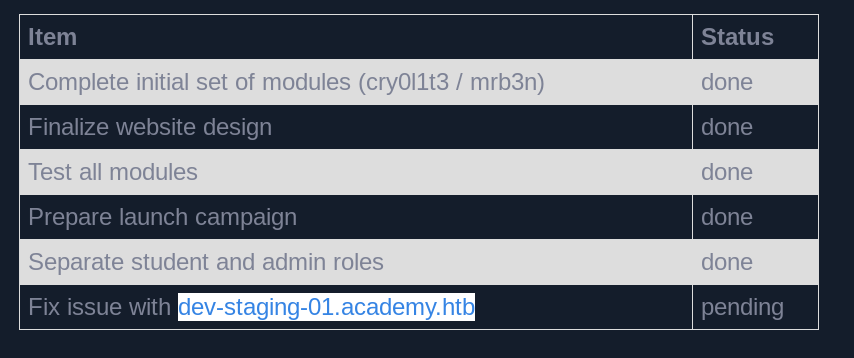
1. Edit roleid parameter to 1 when registering and become admin



1. Login at admin.php site

1. Add dev-staging-01.academy.htb to /etc/hosts

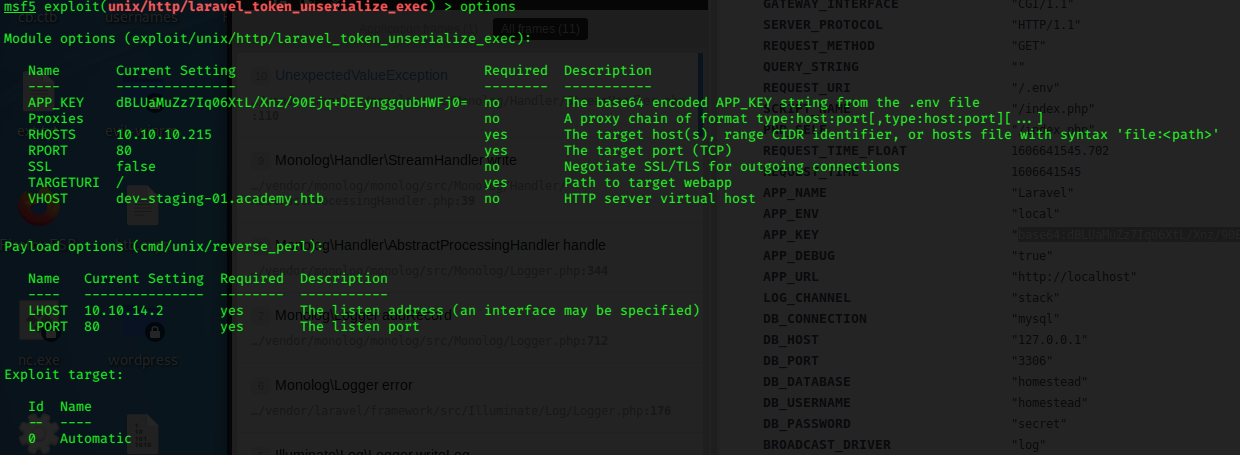


Found sql creds

DB\_USERNAME         "homestead"

DB\_PASSWORD         "secret"

**Priv Esc with Laravel app using Metasploit**



**Users:**

Egre55

Cry0l1t3

21y4d

Ch4p

G0blin

**Results from LinPeas.sh**

Found readable /etc/mysql/my.cnf

!includedir /etc/mysql/conf.d/

!includedir /etc/mysql/mysql.conf.d/

/var/www/html/academy/.env:DB\_PASSWORD=mySup3rP4s5w0rd!!

/var/www/html/academy/.env:DB\_USERNAME=dev

DB\_CONNECTION=mysql

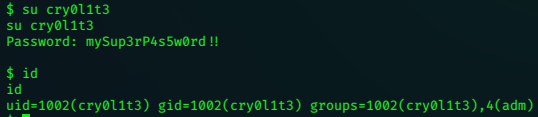
DB\_HOST=127.0.0.1

DB\_PORT=3306

DB\_DATABASE=academy

DB\_USERNAME=dev

DB\_PASSWORD=mySup3rP4s5w0rd!!



hostname': 'academy', 'realname': 'egre55', 'username': 'egre55', 'password': '<REDACTED>'}

cloud-init.log:361:2020-08-07 12:12:07,195 - util.py[DEBUG]: Running hidden command to protect sensitive input/output logstring: ['useradd', 'egre55', '--comment', 'egre55', '--groups', 'adm,cdrom,dip,plugdev,lxd,sudo', '--password', 'REDACTED', '--shell', '/bin/bash', '-m']

**Output with Updated linpeas**

1. 08/12/2020 02:28:10 83 0 ? 1 sh "su mrb3n",<nl>

2. 08/12/2020 02:28:13 84 0 ? 1 su "mrb3n\_Ac@d3my!",<nl>

**PrivEsc with composer**

