The machine wants me to brute force a website, which is locked by a pin.

A screenshot of a cell phone

Description automatically generatedA screen shot of a computer code

Description automatically generatedFirst, I connect using the VPN.

Next, I viewed the site.

A screenshot of a computer screen

Description automatically generatedQuickly testing a basic password of ‘0000’ I get this error message.

The pin code for the website would have to contain the above characters. From 0-9 and A-F, so this means I can use the tool crunch to generate a list of possible passwords.

**3** – min length of password.

**3** – max length of password.

**0-9-A-F** – Character set to be used.

**-o possible.txt** – Save to text file.

Since this is a website-based pin code, I had to acquire some HTML to get it to be brute forced by hydra.

 There most important here is ‘post’, ‘login.php’, ‘pin’. The reason why these are important because they are required to get hydra to function as intended.

-l – means username (don’t need one here).

-P – means password file.

-f – stop hydra after finding correct password.

-v – verbose

http-post-form – HTTP method to use.

/login.php – Website where the pin is submitted.

Pin=^PASS^ - Will replace PASS with values from possible.txt.

Access Denied – Error message to look out for.

-s 8000 – Indicates port

A screen shot of a computer

Description automatically generatedAfter letting it run for a bit, I found the password.

A screenshot of a computer

Description automatically generatedThe flag was found.