Morty at the JuiceShop

by

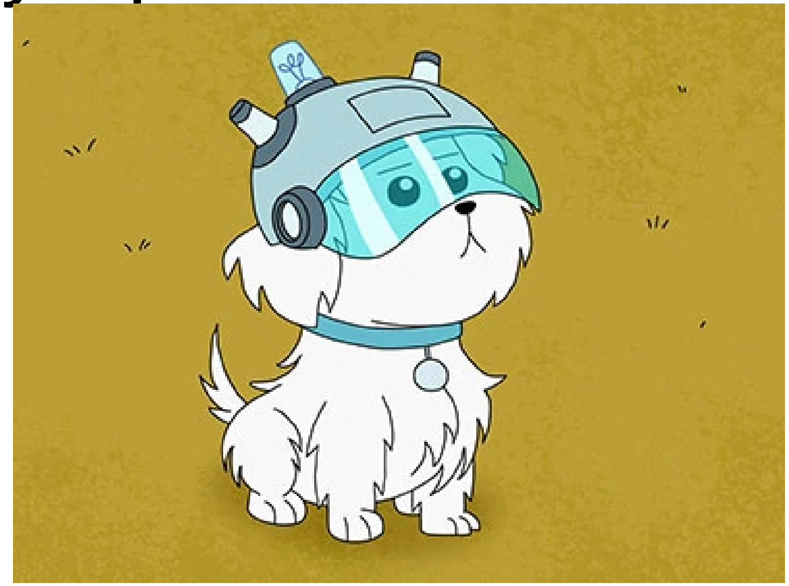
Maurice Cronin

The Challenge

- Reset Morty's password via the Forgot Password mechanism with his obfuscated answer to his security question.
- We have 2 issues to overcome:
  - We only know the (unobfuscated) answer(s) to his security question.
  - The Password Reset mechanism is rate-limited to prevent brute-forcing the answer.

What we do know

- We know Morty’s email
- Morty’s security question (from the reset form):
  - Name of your favourite pet?
- Can be found via google or a friendly nerd
- How Morty’s password is obfuscated (via hints)



Hints

Reset Morty's password via the Forgot Password mechanism

- This password reset challenge is different from those from the Broken Authentication category as it is next to impossible to solve without using a brute force approach.
- Finding out who Morty actually is, will help to reduce the solutionspace.
- You can assume that Morty answered his security question truthfully but employed some obfuscation to make it more secure.
- Morty's answer is less than 10 characters long and does not include any special characters.
- Unfortunately, Forgot your password? is protected by a rate limiting mechanism that prevents brute forcing. You need to beat this somehow.

What we need

- The HTTP return codes for
  - A successful reset
  - A failed reset
  - A blocked reset
- To automate the password reset procedure
- To bypass the rate-limiting mechanism
- To generate a list of possible answers

Tools

- Python
- Web browser – Firefox
- Curl
- Brains ??

Bypass Ideas

- Login as that user before or after triggering the rate limiting mechanism
- Add a null byte to the answer before or after triggering the rate limiting mechanism
- Successfully change another users password via the Forgot Password mechanism
- **Change IP address**

X-Forwarded-For

- X-Forwarded-For header

  The X-Forwarded-For HTTP header field is a common method for identifying the originating IP address of a client connecting to a web server through an HTTP proxy or load balancer.