Kevin Umba

12/09/2022

Capstone Test Report

Group 7

Leaderboard:

The leaderboard has a client side and proxy vulnerabilities. I was able to remove the disable-flag on the leaderboard submit button and trigger the leaderboard without winning a game. I used Burpsuite to proxy the communication between my computer and the server. Then, I intercepted the request to the before it got the server and changed the score to put a fake score.

It seems impossible to prevent people from capturing the traffic on their own computer. However, these solutions could help:

1. Client-side validation: It is not recommended to trust the client to enforce validation because the user has full control. They can change the html and remove any validation as they please. Make sure to add validation on the server side.
2. Server verification and encryption: Using a symmetric encryption algorithm like AES can encrypt the score string in the request. Your server code will use a key to decrypt the string and add it to the leaderboard. Even if a user intercepts the request and changes the score, the server will detect any tampered data.
3. Obfuscation: base 64 encoding or any encoding will not be very useful. It will make the string hard to guess but given enough time, anybody can revert the encoding to the plain text. Encryption is better because the user would have to know the secret key to do anything.

Vulnerability walkthrough:

I am logged in as a user.

Step 1 remove the disabled flag on the html

Graphical user interface

Description automatically generatedA screenshot of a computer

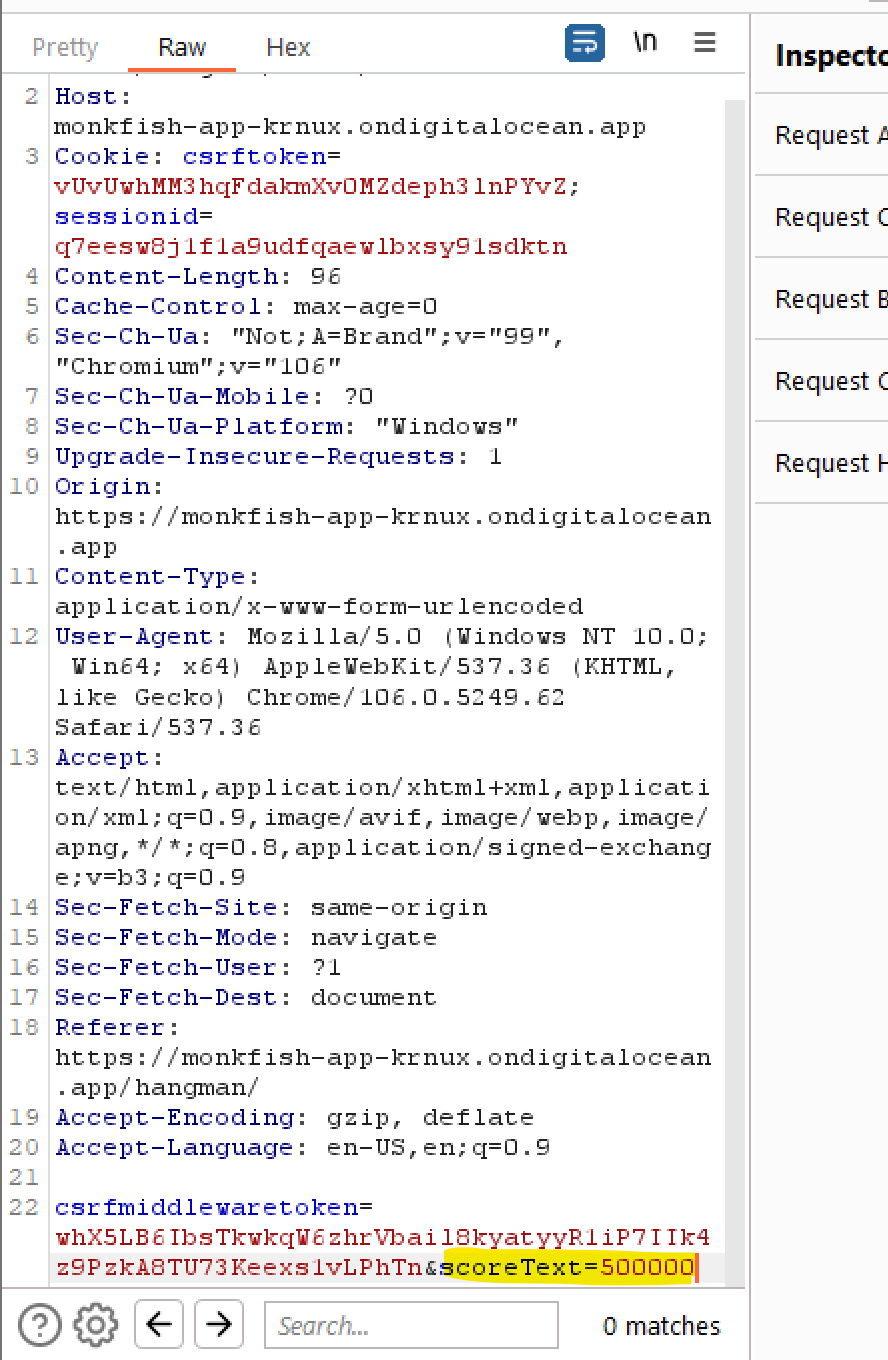
Description automatically generated with medium confidence

Step 2 click on Submit to intercept the request to the leaderboard

Graphical user interface, text, application

Description automatically generated

Step 3 Change the score



Step 4 Check that the leaderboard reflects the fake score

Graphical user interface

Description automatically generated