Off-by-One Overflows

Saturday, October 21, 2017 12:39 AM

- Despite being more rare, buffer overflow vulnerabilities on the web occur when a tier of the application has insufficient memory allocated to deal with the data submitted by the user
- Typically, such a tier would be written in C or a similar language

Solution

- Start by entering in your info and submitting
- There are some hidden forms on the next page
    - Use Chrome Web Developer to reveal them
        - Display Form Details
- We can see that the room number form field has a weakness to 4097 digits
    - 4096 is the maximum it can handle (4 kB)
        - Defined by the programmer
- Create a script to generate 4097 digits of data
- Copy and paste the numbers into the room form field
- On the next page deactivate and reactivate to Display Form Details in Web Developer
- You will now see a data leakage of a bunch of other users on the page due to our successful Off By One buffer overflow attack
- Enter in the name and room number of one of them to complete the challenge