

## 50.020 Security CTF - Challenge

### Group:

Capturing All The Flags

### Members:

Choo Han Ye Samson (1002439)

Tracy Yee Enying (1002379)

Laura Ong Jin Hua (1002464)

Tan How Seng (1002119)

### Category:

Cryptography + Reverse Engineering + Injection Attack

### Challenge Name:

Bob the Builder

### Background:

Bob the Builder wants to build a new home. However, he faces some problems in the process. Help Bob to overcome these problems.

### Part 1:

Bob's family is expanding (he is expecting a new child) and he wants to extend his house. He needs to buy more bricks. His friend sent him a recommendation regarding a website that sells bricks but some parts of the URL was smudged by some mud. Bob needs to find out what is the smudged part of the URL to access the website.

### Details

- The URL that Bob received is `https://<smudged_string>.herokuapp.com/`
- Decrypt the smudged string and append it to the front of the URL

### Hints

- Recall how RSA works:  $c = m^e \bmod n$

When  $n = 735023$ ,

$smudged\_string = 50829\ 295278\ 422602\ 345802\ 90850\ 389841\ 560006\ 595977\ 357704$

When  $n = 999941$ ,

$smudged\_string = 520934\ 30360\ 157684\ 815907\ 560955\ 124923\ 295088\ 331059\ 92786$

- The same encryption is done for each characters separately
- $smudged\_string = c_1\ c_2\ c_3\ \dots$
- Let  $e = 3$

### Part 2:

Bob uncovers the website URL and accesses their website. However, he realised, for the first time in his life, that there were actually different kinds of bricks. But they all looked the same to him and he did not know which one to choose. Help Bob to choose the brick that is most suitable for him by clicking on it.

#### Hint

- The brick sellers will tempt you to buy poor quality bricks by making them more obvious. Look for the non-obvious bricks that are more valuable for Bob.
- Your cursor is your best friend. Don't lose sight of it.

#### **Part 3:**

Bob finds the brick he needs, but realised that it is only sold at a secret underground market. He does not know where to find the underground market, but he heard that a certain "person" has a "secret" file which reveals the location.

#### Hints

- The "person"'s "secret" can be accessed from your current page
- When in doubt, look to the link for clues of the type of attack needed
- The files have standardized names of *subject.object*

#### **Part 4:**

Bob needs to post a request to buy the bricks but the brick sellers refuse to sell the bricks to Bob. They claim that they do not have the authority to sell these limited edition bricks. Only famous establishments like *Capturing all the Flags* have the authority to do so but they are very secretive and difficult to find. Bob refuses to yield because he wants to make the perfect home for his family. Use HTML injection to help Bob buy the bricks by spoofing *Capturing all the Flags* and posting a request to buy bricks on his behalf (you cannot mention the name Bob as the brick sellers still remember him).

The request should look like either of these:

- Samson: <your team name> has been awarded the flag!
- Tracy: <your team name> has been awarded the flag!
- Laura: <your team name> has been awarded the flag!
- How Seng: <your team name> has been awarded the flag!

#### Hint

- Refer to <https://www.w3schools.com/tags/> for a tutorial on HTML tags

#### **Part 5 (optional):**

While building his house and buying bricks, Bob spots a goose approaching him. He recognizes it as Mother Goose, a pet of the fishmonger that lived at the other end of the village. The fishmonger only uses Mother Goose as a means of communication for extremely urgent matters so Bob quickly searches Mother Goose for any messages. He only finds a small scrap of paper at the corner of Mother Goose's mouth. Bob learns that Mother Goose had eaten the message paper. Help him to extract the message from Mother Goose.

### Hints

- This part can be done concurrently (independent of the other parts).
- The message contains important information regarding the flags.
- The message is hidden in Mother Goose using Steganography.
- The key is of length 7, all letters (can be upper/lower case).
- 3 of the letters are {C, T, F} but each of the letters can be in any position