# Generating a 'random' Session ID

Nick Graca

A Background into Computers

- When computers were designed they were supposed to be anything but random
- Imagine using you computer and random actions happen, that would make computers unuseable
- Therefore, computer architects made computers predictable

Computers can't generate truly **random numbers.**

Software still can't manage something as simple as a dice roll.
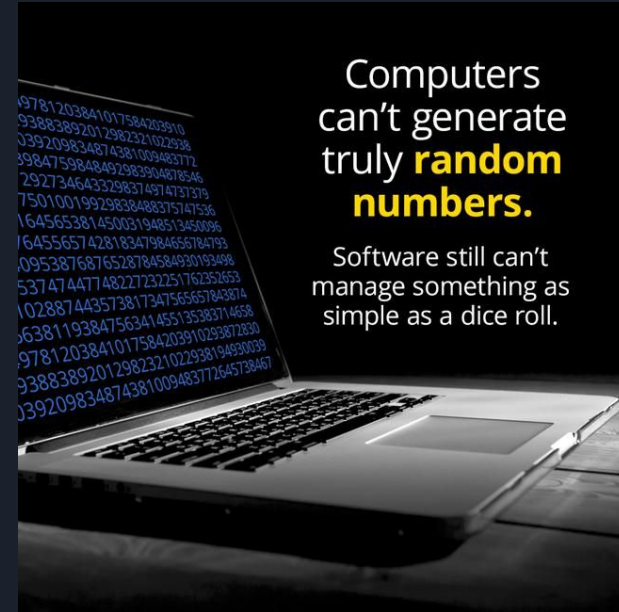
The Problem with Predictability

- Its predictable!
- When generating session id's they need to be random so they can not be guessable
- This is where the problem arises
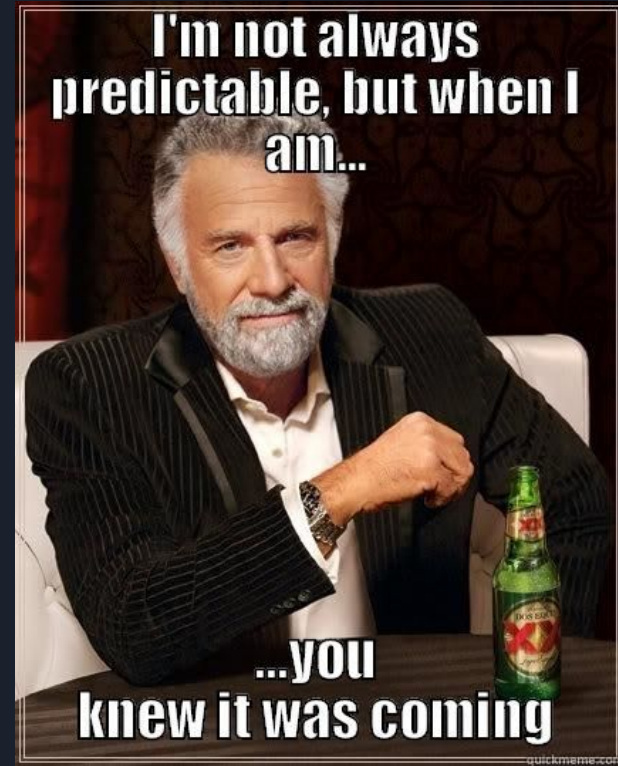
What can be done

- Pretty much every language has a way to generate random numbers however, numbers are not enough, we need letters too!
- I found a great piece of code that does this in php

```php
01  <?php
02
03  $permitted_chars = '0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ';
04
05  function generate_string($input, $strength = 16) {
06      $input_length = strlen($input);
07      $random_string = '';
08      for($i = 0; $i < $strength; $i++) {
09          $random_character = $input[mt_rand(0, $input_length - 1)];
10          $random_string .= $random_character;
11      }
12
13      return $random_string;
14  }
```

What can be done cont.

- That code was better than the built in random number generator because it uses more than just numbers which increases the number of possible values significantly which makes it harder to guess
- You can also specify a length and the longer the string the harder it is to guess
- With just a little bit of code session id's can be much harder to guess

Citations

- Images:
  - http://www.quickmeme.com/img/d2/d2c4f4d5e3d409cde89c88ab96f35aec50b62c4d2f199aac3e5fdea6aad3cbc4.jpg
  - https://dw8stlw9qt0iz.cloudfront.net/KGwWf_ITm-nK0SAAY9tKcAPDei0=/fit-in/650x650/filters:format(jpeg):quality(75)/curiosity-data.s3.amazonaws.com/images/content/meme/standard/94599124-8777-4e95-d18d-630fa35de08e.png
- Code
  - https://code.tutsplus.com/tutorials/generate-random-alphanumeric-strings-in-php--cms-32132