GOOGLE GRUYERE EXERCISE

- **Google Gruyere** (see [http://google-gruyere.appspot.com](http://google-gruyere.appspot.com)) is a platform for simulating attacks against web applications, based on existing vulnerabilities. It showcases various web application vulnerabilities and exploits.

- **Typical exploits include:**
  - Cross-Site Scripting (XSS)
  - Denial of Service
  - Cross-Site Request Forgery (XSRF)
  - Cross-Site Script Inclusion (XSSI)
  - Code Execution
  - Configuration Vulnerabilities
  - SQL Injection
  - Client-State Manipulation
  - Path traversal
  - Buffer Overflow and Integer Overflow

- **Google Gruyere Challenges.** Google Gruyere comprises various challenges (exercises), each of which presents: an explanation of the **nature of an exploit**, some **hints** for carrying out the exploit, and a **fix** for the exploit.

- **Our task.** Attempt the various challenges under each exploit. As much as possible, try and come up with a solution after reading the first hint. Proceed to the second and/or subsequent hint(s) only if you need to see more hints. Attempt these steps before looking at the information available under “Exploits and Fixes”

- **Our learning goal:** to acquaint ourselves with the nature of common web application vulnerabilities, while learning what defenses are available.

- **How to proceed:**
  - Take note of the **warning** at [http://google-gruyere.appspot.com](http://google-gruyere.appspot.com).
  - Read the information available at [http://google-gruyere.appspot.com/part1](http://google-gruyere.appspot.com/part1)
  - Setting up: go to [http://google-gruyere.appspot.com/start](http://google-gruyere.appspot.com/start)
  - Write down your instance ID and read the “terms of service”. Click on the “Resume” link and sign up as a new user.
  - Sign in and proceed with the various parts (2 ... 5). Starting from Part 2 ([http://google-gruyere.appspot.com/part2](http://google-gruyere.appspot.com/part2)), complete each exercise (challenge) after reading about an exploit.