Task 1 - Test the buggy application

- http://goalsec.com/exercise_2017/

Bug list

General

Credentials

- typo - "You" -> "Your"
- not sure - credentials are not capitalized
- strange commented line - `<!--Argh!!! What am I doing???!!!!-->`
- not valid behavior for unicode characters: ** č, ď, ľ, Í.. -> & (special characters are transferred to UTF-8 key-codes which usually begin with '&#')
- no checking for whitespaces in front of name and last name - results in credentials not being shown
- not sure - from time to time - not the same results for the same inputs

Input string

- input - `&#72;&#101;&#108;&#108;&#111;` is interpreted and results into "Hello"

Standards

HTML5

- using unsupported HTML5 property "align" in h1 tag

Security

Conventions

- using not recommended form method "get" for personal data.

XSS - Cross-site Scripting

- HTML code is not escaped http://goalsec.com/exercise_2017/index.php?firstname=%3Ch1%3EHello%3C/h1%3E&lastname=%3Ch2%3EWorld%3C/h2%3E
- javascript code is not escaped http://goalsec.com/exercise_2017/index.php?firstname=%3Cscript%3Ealert(%22Hello%20World%22);&lastname=%3C/script%3E

Other mitigation methods

- Cross-Site request forgery
- SQL Injection
- Stressing - how the app responds when dealing with many users