CSE 3101: Internet Computing II

Lab Session 4

Paul Crawford

Semester 1, Week 9 (22nd & 23rd October, 2018)

1. Aims

1.1. Further understanding of client-side Web Forms and the server-side PHP language.

1.2. Further increased facility with the ongoing sets of concepts & techniques needed for eventual completion of future Assignments; in particular, the sanitising/validation of submitted data.

2. Tasks

2.1. Web Forms — Validation (Upon Submission) {Server-Side}

2.1.1. Work through the examples of server-side Form Validation, Required-Fields Handling, & Name-/URL-/Email-Field Handling (via *regular expressions*) available at the **W3Schools** site's PHP tutorial, § 'PHP Forms'.

2.1.2. Practice applying such data validation in (the respective processing pages for) the web forms from *Lab Session 3*, and/or strengthen the handling of those in your own *Address Book* web app.

2.2. Processing Pages / Handlers — Database-Related Validation {Server-Side}

2.2.1. Work through the examples of Prepared Statements (guarding against SQL Injection) available at the **W3Schools** site's ~~SQL~~PHP tutorial, § 'MySQL Database'. Alternatively, you could explicitly validate SQL parameters using *regular expressions*.

2.2.2. Practice applying such data validation in the processing-pages from *Lab Session 3*, and/or strengthen the handling of those in your own *Address Book* web app.

2.3. Overall Considerations

2.3.1. For additional practice and code samples, you could also explore any of various useful tutorials & references available online. For instance, there are several PHP and SQL interactive examples available at the **W3Schools** site (<w3schools.com>); pay special attention to the sections on *security and validation*. Likewise, the official **PHP Manual** (<secure.php.net/manual>) has information on *SQL vulnerabilities* (§ 'Security > Database Security > SQL Injection') and *regular expressions* (§ 'Function Reference > Text Processing > PCRE'), etc.