# School of Creative and Digital Industries

# Open Source Systems CW2 Critical Evaluation: Academic Year 2021 to 2022

|  |  |  |  |
| --- | --- | --- | --- |
| **Module Title:** | Open Source Systems | **Module Code:** | CO551 |
| **Assignment No/Title:** | CW2 | **Assessment Weighting:** | 50% |
| **Submission Date:** | 18/05/2022 | **Feedback Date:** | 3+weeks |
| **M****odule Tutor:** | Jonathan Jackson | **Degree:** | MSci. (Hons) Cyber Security |
| **Student Name:** | **Kate Gordon** | **Student ID:** | **21802875** |



8382325

Please mark according to Guidelines

<http://bucks.ac.uk/marking_guidelines>

**CO551 Open Source Systems Critical Evaluation**

**By**

**Kate Gordon 21802875**

**Of**

**Buckinghamshire New University**

This critical evaluation will assess two server-side approaches to development and two security concerns in relation to managing personal data. The two server-side approaches this critical evaluation will assess are PHP and HTML. The two security concerns that will be assessed by this critical evaluation are unauthorised access and unauthorised code alterations.

The PHP approach to development has evolved over the last 20 years. PHP frameworks have facilitated better web programming according to Benmousa *et al.* (2019). It opened up the world of open source development to everyone with an interest in programming and web or web application development.

Carter (2014) explains that HTML or HyperText Markup Language has many frameworks that disguise the intricacies of client and server-side development, this leads to a lack of knowledge and understanding of the extensive aspects of the foundations to web applications.

Unauthorised Access can be mitigated by introducing access rights and ensuring that only those who need the full data collection can access it.

Unauthorised Code Alterations Via Inspect can be mitigated to an extent through the use of validation. It can also be combatted by removing the gibberish code and restoring the infected files from an uninfected backup.