THE UNIVERSITY OF SYDNEY

INFO2315 Assignment 1

Due: During your Tutorial in Week 7, Semester 2 2017

This assignment is worth 3% of your final assessment

Over the last few years numerous Australian government services have seen an increase in cyber attacks, data breaches, and general nefarious behavior as more and more of their systems are transitioned to electronic or web based platforms. In this assignment you will be building a website based off current on-line government services.

Task description

You will be required to implement the following features using Python's bottle and pycrypto packages along with any core packages.

- Users must be able to register and log in
- Differing levels of access for user, staff and administrator accounts
- The ability to upload and view appropriate details and documentation for users
- Users must be able to submit applications for processing by staff
- Staff must be able to view and process applications submitted by users
- Administrators must be able to view and edit user details
- All uploaded information must be stored in a persistent manner (restarting the Python application reloads data from previous runs)
- Administrators must be able to clear the 'database' to a default state
- A persistent audit or log of all behavior on the site, viewable by administrators

Due to the particular requirements of government departments, all users must be anonymous to the administrators, but not the staff. In order to achieve this particular security goal, user logins are handled by assigning individual ID numbers that are used for authentication.

In addition to these requirements, your group must select **one** of the following options.

Medicare

The Australian health care system was subject to scrutiny earlier this year after Medicare card numbers were found for sale on line. This system contains 1) health records, registration of doctors and other medical professionals, 2) manages and tracks prescription medicine and; 3) controls the payment of rebates for medical expenses. Were this system to be exploited, prescription drugs could be acquired by those who do not necessarily need them, people could be listed with disabilities that they do not necessarily have, and rebates could be claimed for appointments that never occurred and were never paid for.

- Users must be able to register as either a member of the public, or as a medical professional
- Users must have a unique Medicare number that is not disclosed to any unauthenticated users
- Medical professionals must be able to log an appointment and append details to a member of the public's record
- Medical professionals must be able to prescribe medication for users, include information such as number of repeats and whether a rebate may be claimed on this
- Users must be able to request rebates based on appointments or prescriptions
- Staff must be able to approve or deny requests for rebates

For more details see:
Medicare card numbers 'being sold on dark web'

The Census Site

Last year the Australian Bureau of Statistics moved the census to an almost entirely on line platform with disastrous results. Through a combination of outsourcing, poor planning for the sheer number of users, and a few legitimate denial of service attacks, the census was unavailable for hours at a time on the day that it was supposed to be completed. It is still not clear if any private details were stolen or leaked.

- Users must be able to register as a member of the public or as a researcher
- Users must have a unique census ID that is not disclosed to any unauthenticated users
- Members of the public must be able to enter their census response details anonymously, the questions listed should closely mimic those found on the actual census
- Staff must be able to verify a member of the public's completion of the census, without seeing their input
- Researchers must be able to see aggregate data without viewing individual responses

For more details see:
2016 Sample Census Australian Bureau of Statistics says website attacked by overseas hackers
Possible hack of private information cannot be ruled out, experts say
ABS website not attacked or hacked, Michael McCormack says

Births, Deaths and Marriages

A number of fundamental authentication issues have been found with the Australian registry of births, deaths and marriages. In some ways these documents are the ultimate proof of identity however there is next to no formal authentication on who is granted the authority to produce birth and death certificates. The potential ramifications of creating a birth certificate, or a fraudulent death certificate for a Prime Minister, or indeed any member of the public is a matter for serious consideration.

- Users must be able to register as either a medical practitioner, marriage officiator or funeral director
- Marriage officiators must be able to upload details for weddings, such as the time, place and participants
- Staff must be able to process and either approve or reject marriage certificate applications
- Marriage officiators must be able to upload details for divorces, such as the time, place and participants
- Staff must be able to process and approve divorce applications, and revoke the appropriate marriage certificate
- Medical practitioner must be able to upload details for births, such as the time, place, name of the infant and relatives
- Staff must be able to process and either approve or reject birth certificate applications
- Medical practitioner must be able to upload details for deaths, such as the time, cause and whether an autopsy was performed
- Funeral Directors must be able to upload details about family members and next of kin
- Staff must be able to process and either approve or reject these applications and decide whether a coroner or investigation is required.

For more details see:
Melbourne hospital reports 200 patients as dead instead of discharged
Defcon 23 Presentation on exploiting the "Death Industry"

The Road Transport Authority

As Sweden has seen recently, leaking the license details of the entire country's motor registry can have consequences for military and intelligence agencies. Other exploits can lead to attackers granting or revoking parking tickets and licenses, transferring ownership of vehicles into their own name, listing vehicles as having been destroyed when they haven't, or triggering audits on individuals through similar processes.

- Users must be able to register as either a member of the public, or a road safety officer

- Members of the public must be able to apply for a license
- Staff must be able to approve or reject license applications and issue members of the public with a license number
- Road safety officers must be able to issue vehicles with fines and demerits
- Members of the public must be able to register a vehicle in association with themselves
- Members of the public associated with vehicles must be able to pay fines and view their merit points
- Staff must be able to approve payments and revoke licenses
- Members of the public must be able to apply to renew their license
- Staff must be able to approve or reject license renewals
- Members of the public must be able to notify on the sale of a vehicle including the purchaser and the amount
- Staff must be able to approve or flag for investigation on the sale of a vehicle
- Members of the public must be able to list a vehicle as destroyed
- Staff must be able to approve the destruction of a vehicle
- Destroyed vehicles cannot be re-registered or sold

General Details

SQL is not required for this assignment, manage user data as Python objects. Please do not copy official government logos and iconography for your site. All features are required to be persistent: shutting down and restarting your Python server should reload your data from an external file, though administrators are required to have a button that will reset the site to a default state.

Assessment Criteria

You will present and demonstrate your site to your tutor during your tutorial. You will be expected to answer questions about the design and security of your site.

You will be marked out of 10 for this assessment task.

- A mark out of **2** for correctly meeting the specification. A mark of less than 1 indicates that most of the specification was incomplete or non-functional. A mark of 1 to 1.5 indicates that most of the specification was complete and functional and that data is stored in a persistent manner. A mark of 2 indicates that the specification was complete, functional and realistically models behavior that would be observed in the real system.

- A mark out of **2** for the presentation of the site (navigation between actions and layout of components). A mark of less than 1 indicates a simple static page that does not allow navigation between the different procedures of the website and does not facilitate useful feedback to the user about their activities. A mark of 1 to 1.5 indicates some appropriate layout of the site, allowing navigation between procedures, but lacks feedback on the stages of each procedure. A mark of 2 indicates a presentation of the site that could be found in a real implementation, interactive, well composed layout, easy to use. Students aiming for the highest score would employ HTML, CSS and other web technologies. Information available from: HTML W3schools CSS W3schools. It bears repeating that students should not copy or rip real government iconography for their own sites.
- A mark out of **4** for security features you have implemented 1 mark for correct password management and preventing the use of weak passwords (including passwords that are too similar to user details). 1 mark for secure ongoing authentication. 1 mark for appropriate permission controls. 1 mark if your tutor cannot break your site.
- A mark out of **2** for any appropriate additional features you have added to the site. This can include features such as uploading, storing and retrieving documents (such as pdf files) or images in addition to (not a replacement for) text or other appropriate fields. You should bring your tutor's attention to any such features you have added.

Submission Details

The following details should be read carefully regarding the submission of this assignment

Group Assessment Forms

The following form must be completed and submitted to your tutor on the due date (electronic or physical):
http://sydney.edu.au/engineering/it/current_students/undergrad/guidelines/assignment_sheet_group.pdf

Each member must list their contribution percentage next to their name. When the total percentage is 100%, each group member must sign to agree. The marks awarded will be proportional to the contribution of the group member. If the contribution is not 100%, or there are disagreements about contributions, the assignment will not be graded until it is resolved.

It is important to discuss the distribution of work and expected contribution of each member as early as possible. At any time group should bring discussions about progress and issues they are experiencing to the attention of the group. The group members should cooperate and assist one another where possible.

Code Submission

In addition to presenting to their tutor during the tutorial, one member of each group will be required to submit their site to Edstem as a single zip file: https://edstem.org/courses/599/assessments/1079. They must also fill out the group.txt document with appropriate details.

If you have any questions, or are unsure about the submission process or any aspects of this assignment, please ask sooner rather than later!

Academic declaration

By submitting this assignment you declare the following:

I declare that I have read and understood the University of Sydney Student Plagiarism: Coursework Policy and Procedure, and except where specifically acknowledged, the work contained in this assignment/project is my own work, and has not been copied from other sources or been previously submitted for award or assessment.

I understand that failure to comply with the Student Plagiarism: Coursework Policy and Procedure can lead to severe penalties as outlined under Chapter 8 of the University of Sydney By-Law 1999 (as amended). These penalties may be imposed in cases where any significant portion of my submitted work has been copied without proper acknowledgment from other sources, including published works, the Internet, existing programs, the work of other students, or work previously submitted for other awards or assessments.

I realise that I may be asked to identify those portions of the work contributed by me and required to demonstrate my knowledge of the relevant material by answering oral questions or by undertaking supplementary work, either written or in the laboratory, in order to arrive at the final assessment mark.

I acknowledge that the School of Information Technologies, in assessing this assignment, may reproduce it entirely, may provide a copy to another member of faculty, and/or communicate a copy of this assignment to a plagiarism checking service or in-house computer program, and that a copy of the assignment may be maintained by the service or the School of IT for the purpose of future plagiarism checking.