**Website security**

**Access**

To access the Food Bank website the user must have a username and a password that may be obtained in the user registration process.

**Registration**

The systems administrator who is appointed by the Board of Trustees oversees the user registration process. The volunteer coordinator decides the level of access for each new user and will advise the systems administrator. The registration process may be carried out by any user authorised to do so.

The password is encrypted with SHA1() which is a PHP function to encrypt the password in a hash which is then put in the database with the new user details.

**Authorisation**

There are different types of authorization in the website, the authorisation for each user is determined by the volunteer coordinator. The level of authorisation determines which features of the website are visible.

The types of user are:

**Admin:** systems administrator, appointed by the Trustees, The admin has full access to the entire system.

**Agency staff:** Staff working at one of the referral agencies. The Agency staff is enable to read and modify the client database, read the location of each warehouses, distribution points and agency locations, and read and modify the voucher database.

**Packer:** Works in the warehouse packing parcels. The packer is enable just to read the items database.

**Counter:** Works in the warehouse counting items in the system. The Counter is enable just to read and modify the items database.

**Distribution Point Staff:** Works in the distribution point and is responsible for exchange vouchers for parcels. The distribution point staff is enable to just read the client database, just read the parcel database, just read the location of each warehouses, distribution points and agency locations, and read and modify the voucher database (except create new ones).

**Volunteer Coordinator:** Responsible for register, accept, modify and delete volunteers registrations. The volunteer coordinator can modify and read the user database (register new user, modify existent users, delete users, enable users, etc.).

**Trustee:** The trustees is responsible for the legal part of the charity organization. The Trustee is enable to read the donation database, read the items database, and report problems.

The levels of information that can be accessed are:

**Client:** only admin, agency staff and distribution point staff can access.

**Donation:** only admin and Trustee can access.

**Food Items:** only admin, counter and trustee can access.

**Food Parcels:** only admin, distribution point staff and counter can access.

**Location:** only admin, distribution point staff and agency staff can access.

**Reports:** only admin and trustee can access.

**Vouchers:** only admin, distribution point staff and agency staff can access.

**User Control and Register:** only admin and volunteer coordinator.

A user’s level of authorization can only be changed with the approval of the volunteer coordinator.

The system administrator needs to be added directly to the database and has unrestricted access to any website resource. In addition, an admin is able to register new admins.

**Risks**

Both the systems administrator and the volunteer coordinator are the most powerful in terms of security in the Canterbury Food Bank website because they are able to accept new volunteers or change the level of authorisation of each one. Therefore, the volunteer coordinator and the systems administrator need to be trustworthy because they are able to allow access to confidential information.

Thus, the risk in this layer of the website is the authorisation. A person should only be authorized to see confidential data by trusted users. The encryption of passwords creates a cryptographic barrier to prevent unauthorized access to the website.

**PHP**

According to the CVEDetail, the PHP 5.5.6 was evaluated as follow:

The scan function in ext/date/lib/parse\_iso\_intervals.c in PHP through 5.5.6 does not properly restrict creation of DateInterval objects, which might allow remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted interval specification.

* Confidentiality Impact: None (There is no impact to the confidentiality of the system.)
* Integrity Impact: None (There is no impact to the integrity of the system)
* Availability Impact: Partial (There is reduced performance or interruptions in resource availability.)
* Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit. )
* Authentication: Not required (Authentication is not required to exploit the vulnerability.)
* Gained Access: None
* Vulnerability Type(s): Denial Of Service Overflow

**Risks**

The denial of service attack consists in the simultaneous access to a target website by thousands of users, making the access extremely slow or even unavailable the access to the website. This kind of attack to the Canterbury food bank is quite unlike to happen, because of nature of the Canterbury Food Bank Website, there is no point to unavailable the site.

There are many ways to prevent a denial of service attack, some of them are:

* The firewall can be set up to avoid access from unusual IP addresses.
* Using switches and routers with some rate-limiting.
* Using Application front end hardware, that is a hardware that works together with routers and switches that can analyse packets and identify malicious ones.

**MySQL**

We are using the version MySQL 5.5.34 and I could not find a proper security issue that has not been fixed in my research in internet. However, According to CVEDetail, in the following link,

<http://www.cvedetails.com/cve/CVE-2013-3812/>

, the last vulnerabilities evaluation concerning the last versions and previous versions of MySQL, except some version as, for example, the 5.5.34, according to the list showed in the link above.

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.31 and earlier and 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Replication.

* Confidentiality Impact: None (There is no impact to the confidentiality of the system.)
* Integrity Impact: None (There is no impact to the integrity of the system)
* Availability Impact: Partial (There is reduced performance or interruptions in resource availability.)
* Access Complexity: Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)
* Authentication: Single system (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).)
* Gained Access: None

<http://www.cvedetails.com/cve/CVE-2013-5807/> :

Unspecified vulnerability in Oracle MySQL Server 5.5.x through 5.5.32 and 5.6.x through 5.6.12 allows remote authenticated users to affect confidentiality and integrity via unknown vectors related to Replication.

* Confidentiality Impact: Partial (There is considerable informational disclosure.)
* Integrity Impact: Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
* Access Complexity: Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
* Authentication: Single system (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).)
* Gained Access: None