centercode

Centercode Platform

Security Overview

Prepared by

Neil White

CTO, Centercode

v14 released 07-2014

Table of Contents

Introduction

Due to the highly confidential nature of Customer Validation testing, Centercode has taken serious measures to ensure the security of all data contained within the Centercode Platform. This document outlines many of the security measures and methodologies utilized throughout the Centercode Platform.

Many of the security measures covered within this document are in the form of custom solutions developed by Centercode to meet the strict and unique requirements of a User, Team, and Project based collaboration tool. While some measures are inherently available, others (such as Project Passwords) are based on administrator preference.

The final sections of this document offer a brief overview the network infrastructure driving the Centercode Platform, as well as the methodology used in maintaining it.

Questions and Feedback

We take great pride in the level of security offered throughout the Centercode Platform. We encourage you to send any questions or comments you may have to security@centercode.com, or contact us at **(800) 705-6540.**

Definitions

Centercode – Centercode's hosted web-based Customer Validation software.

Centercode Platform – The complete Centercode infrastructure including application, database, and file servers, in addition to proprietary processors and network infrastructure.

Community – A collection of Users, Projects, and Resources which compose an Implementation. The Community is the highest tier Scope in Centercode.

Community Manager – A user with roles which grant them complete control over the Community Scope, including the ability to create other administrative (Community or Project Manager) users.

Implementation – An instance of Centercode dedicated to an individual customer. Each Implementation includes one Community and multiple Projects and Users. Each Implementation equates to a single database.

Rackspace – Centercode's hosting provider. Rackspace is a large national co-location facility. See www.rackspace.com

Manager – A user licensed to administrate the structural nature of either a Centercode Community (*Community Manager*) or Project (*Project Manager*). Managers are granted the highest levels of access in Centercode.

Participant – An end-user (commonly a tester or customer) within a Centercode Implementation. Participants have access to view resources and provide feedback (as defined by Managers).

Project – A collection of Users, Resources, and defined access roles within a Community. Projects include their own set of custom dynamic Teams and Roles which grant further access, and each represent a single Scope.

Project Manager – A user with roles which grant them complete control over their own Project(s) Scope(s).

Project Team Member – An employee or vendor participating within a Centercode project. Project Team Members generally maintain greater access than Participants, including the ability to view all feedback, moderate user forums, and generate custom reports.

Scope – An entity within Centercode that includes its own set of Users, Teams, Roles, and Resources. The Community and each individual Project represent a unique Scope.

SLA – Centercode's Service Level Agreement which mandates uptime and support of the Centercode Platform. Available at www.centercode.com/sla/

Team – A named set of Users which are granted Roles to provide access to features or information. Unique custom Teams exist at the Community and Project levels.

User – Any user with an account within a Centercode Implementation.

I. Standard Application Security

1. Centercode Login Process

Access to the Centercode application is granted via a custom proprietary login and authentication engine. Each user is given a unique Login name and Password of their choice. Upon login (validation of Login and Password) users are given access to a list of only those Projects currently available to their personal account.

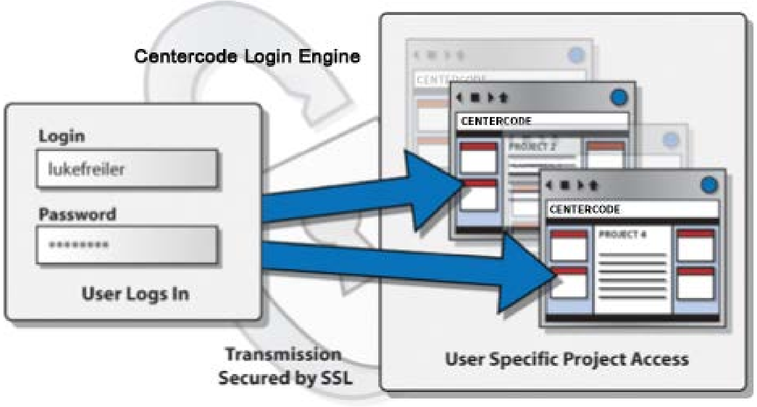

Figure 1: Centercode User Login

Login Details:

- Centercode Passwords are a minimum of six characters long by default, but the criteria for passwords can be configured to match policies set by a Community Manager (via a custom regular expression string).
- Passwords are stored in encrypted form (AES/128 bit) using a hash of their complete login credentials.
- Passwords cannot be retrieved or viewed by anyone, including Centercode (but can be reset by a Community Manager).
- By default, users may attempt three invalid password attempts before their account is locked for a short period of time (eliminating brute force/dictionary hacks).
- Any changes to personal account will email the user to inform them of the change, raising their awareness of any unauthorized changes.

Password Retrieval Security

- Passwords may not be retrieved (and are never sent) via email.
- Passwords may only be reset using the site and its secured connection.
- Password reset emails send out a one-time use key which can be set to expire.

2. Secure Socket Layer (SSL) Access

All Centercode projects are accessed through a TLS secured web interface. This interface ensures that all data (including login and feedback information) is encrypted when being sent to or from the web client and Centercode servers. This level of security ensures that rogue users "sniffing" internet IP packets do not have the ability to acquire meaningful data (in the case of most sites this includes credit card and personal information, in the case of Centercode it includes all traffic). This only exists for customers that use a *.centercode.com domain or if the customer supplies a SSL certificate to us for their custom domain.

SSL Implementation Details:

- 256 Bit SSL Encryption is utilized.
- Non-secure links (**http://**) are automatically redirected to SSL equivalents (**https://**).

3. Role and Team Based Security

Centercode includes a powerful Role based access engine, allowing Manager level individuals to define access to an enormous array of elements and information at two primary scopes:

1. **Community** - Implementations include a single named Community
2. **Project** - Implementations may include any number of Projects within a Community

The following are a few of the common areas with Role based access control:

- Community Administration
- Community User and Team Administration
- Community Reporting
- Community Forms (User Profiles, Test Platforms, Surveys)
- Community Content
- Project Administration
- Project User Administration
- Project Feedback Types
- Project Versions, Builds, and Patches
- Project Task Lists
- Project Content
- Project Tools (Knowledge Base, Email Tools, etc.)

The Centercode Role engine offers the ability to present Users with highly customized experiences tailored specifically to meet their needs and responsibilities.

Role and Team Based Security Details:

- Teams exist on two distinct Scopes (Community, Project)
- Teams are identified by *Team Type*, which both restricts and enforces access to specific roles (ensuring Managers can always access administrative functionality, and Participants cannot access inappropriate administrative functionality)
- Every Project has its own set of dynamic Roles and Teams
- Project Teams and Roles may be standardized and built into Project Templates
- Any number of Teams may be created
- Users may belong to multiple Teams
- Teams may include any number of users

4. Page Based Security

Centercode uses a per-page-based security scheme to ensure each User has appropriate access to any page which they attempt to access. This scheme is used when both linking to and moving throughout the site. As a user moves from page to page, user security access is checked prior to loading every individual page. This ensures that users attempting to access unauthorized pages (for instance by changing values in the URL) will not succeed. Every action taken within the Centercode application is logged as a page hit within the user's session.

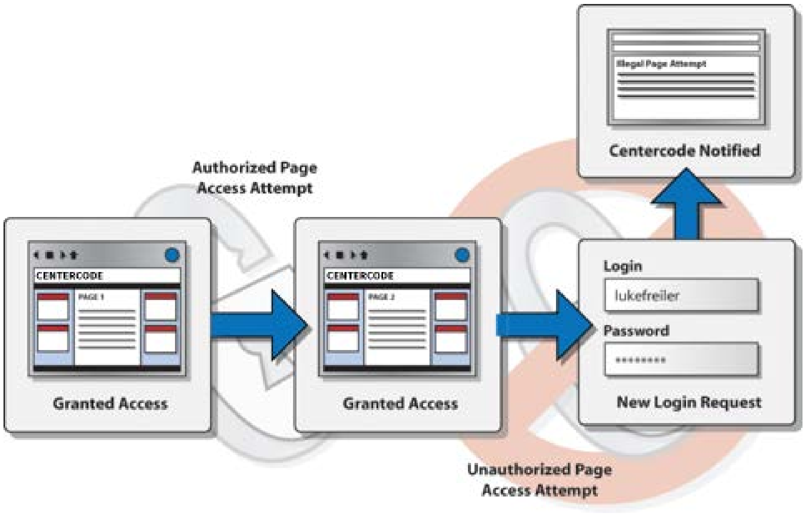

Figure 3: Page Based Security

5. External Linking

Centercode always allows external linking (for instance from an automated email message or browser bookmark), but ensures that proper authentication will be followed no matter which page is requested. When attempting to link to a project page from any unauthorized source, Centercode will allow a user to present login credentials. Only upon approval will users be redirecting to the correct page.

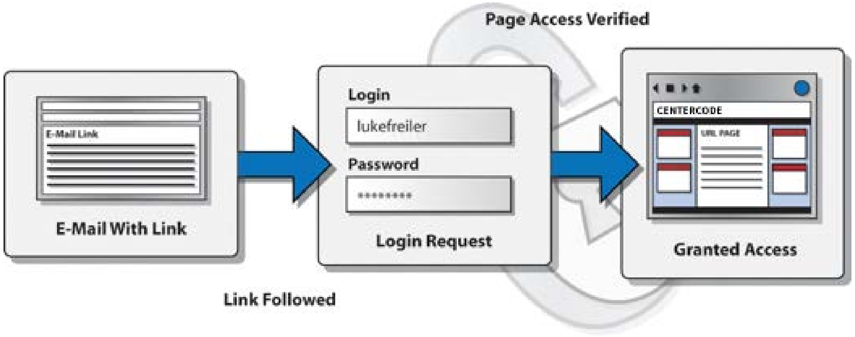

Figure 4: External Linking Methodology

6. File Download Protection

Files hosted on the Centercode Platform may not be referenced by direct linking, unless explicitly allowed by a Content Manager. Centercode employs four levels of file security throughout the application. Most areas of the application employ a minimum of **Medium Security** level, while key areas (such as Release Management) allow the Manager flexibility to determine what level of download security is appropriate.

High Security

The High Security download type requires a user to be logged in, the file link is only valid for the current session and the link to the file that was presented to any user is only accessible by that user (no bookmarking and no link sharing). The download and user attempting download are logged. Few client download managers are supported because they must operate within the context of the user’s browser to share cookies and session with the browser.

Medium Security

Like High Security, Medium Security requires a user to be logged in, but the file link can be bookmarked or copied for later access. This link cannot be shared between users, and can only be used by the original user. The download and user attempting download are logged. Some client download managers are supported.

Low Security

Similar to Medium Security a user must be logged in, however the file link can be bookmarked and can be shared between application user accounts. The download and user attempting download are logged. With each security level various download managers are supported. This level of security supports most managers that allow for HTTPS file download, and that support secured resources (username/password protected resources). This security level is also often used to reference files within other areas of the application (such as Videos, Logos, Screenshots, etc.).

No Security

The lowest of the file download types allows sharing of file download links, with both users and non-users of the application. This security type is most like a typical Internet upload, however the download attempt is logged and associated with an anonymous user. Because a login is not required most download managers are supported.

Common to all four download types, direct file paths are never distributed via Centercode or its automated functionality. Instead, links are provided through a secure file proxy where individual user access is verified prior to serving any file.

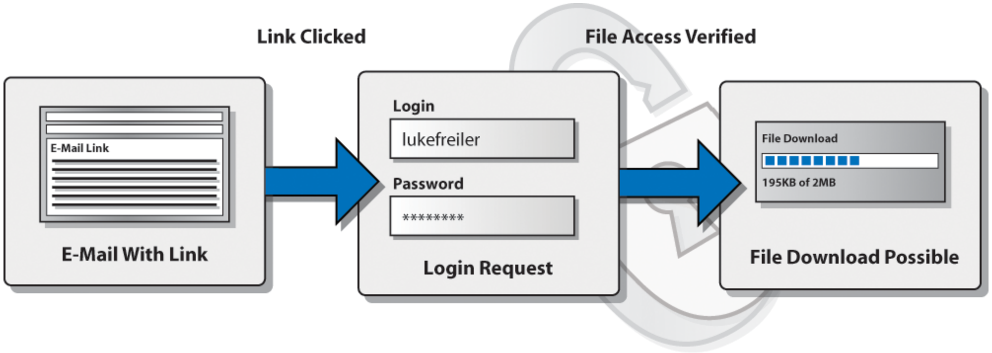

Figure 5: File Download Protection

Details on File Downloads:

- An additional level of security may be added by encrypting files prior to uploading them to Centercode.
- Users are granted access to individual files based on standard Centercode Roles.

7. URL / Form Encryption

All unique identifiers which are visible to end-users utilize 16-byte GUID's (Globally Unique Identifier) to further ensure that changing values will not result in access to unauthorized data. This ensures users have no ability to "guess" at values.

GUID Example: **0DB3B55F-AF79-4524-BC4C-32D554696D28**

Note that this is an additional level of protection over Centercode's standard page based security. In the event that a user was to guess a valid ID string, the standard security scheme would cross check user authorization on that new page, denying access when appropriate.

8. Cross Site Scripting (XSS)

Centercode works to ensure that end users are not able to enter functional HTML or JavaScript of any kind, which would result in uncontrolled scripted actions. URL, form tampering and data manipulation is prevented.

Managers however are allowed this ability for the purpose of being able to further personalize the application to meet their needs, but only available in the manager specific areas. For example, a Manager can add JavaScript to each page to track activity within an external tool such as Google Analytics. Managers may also add HTML to many resources to further their branding of the application and ensure a uniform look and feel throughout the application, however they will not be able to add HTML to forms submitted outside of the manager-only areas.

9. Cross Site Request Forgery (CSRF/XSRF)

CSRF attacks are designed to 'trick' an unwitting user into performing a malicious, mischievous, insecure, or destructive action.

As a simplistic example of this type of attack, consider the following scenario: an attacker distributes an email message to known Centercode users. This email message contains an embedded HTML image tag that loads a page within Centercode. If the loaded page were capable of, for example, removing a vital resource from the system the simple act of the right user viewing such an email could have devastating repercussions.

Centercode architectural standards include methods to mitigate the potential damage these attacks could inflict.

10. Customer Data Separation

Every Centercode implementation utilizes its own distinct database. In addition, data entered into the Centercode application is transported through strictly controlled pathways that are designed to manage the flow of this data from end to end. This mechanism ensures information associated with one resource is not inadvertently associated with any other resource.

Maintaining the integrity and security of files that are uploaded to the Centercode application is just as important as other information that is maintained within the application. All uploaded files are stored in separate folder paths that are dedicated to one specific customer. Each file is located within the file store using various points of information stored with the application data, blending the file integrity and security mechanisms with the data integrity and security mechanisms previously detailed.

II. Optional Security

The following items offer an additional optional level of security for Centercode implementations.

1. Additional Team-Based Community and Project Passwords

In addition to the standard levels of security used throughout Centercode, additional passwords may be required on a team-by-team basis at both Community and Project levels. This allows Community or Project managers to offer an additional level of protection for specific teams who may have access to highly sensitive information or tools.

For example, a project manager could require an additional password upon entry into a project by anyone internal to the company (such as engineers and marketers), thus having access to view more sensitive data than other users such as testers.

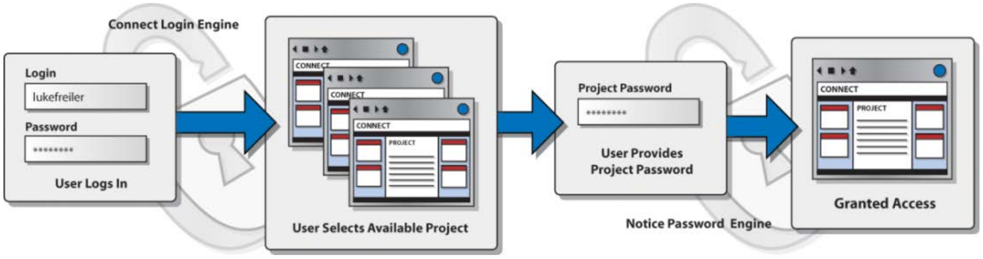

Figure 6: Project Passwords

2. Notices (Legal Agreements, Blocks, etc.)

Centercode's Notice engine may be used to ensure users see and/or agree to specific information. This includes items such as privacy notes and legal agreements. This simple step helps ensure users understand the importance and secure relevance of the information they have access to, thus reducing chances that users will act irresponsibly. These are shown to the users prior to gaining access to the level.

3. IP Geo Location Filtering

Centercode holds a database of IP locations that you can then set by country or individual IP address to block devices coming in on those IP addresses. You can choose this at the Community and/or Project Scopes and will block (or allow) them accordingly.

III. Centercode Platform Infrastructure

1. Firewall Filtering

Traffic on all but essential ports is filtered out prior to connection to any server. Traffic is consistently monitored with automatic reporting notifying Centercode staff of any potential illegal entry attempts.

2. Database Servers

The Centercode Platform utilizes Microsoft SQL Server 2008 R2 for all database functionality. Direct access to database services by systems that are not physically located on our network is prohibited by rules set on our firewall. Database servers are locked down using various security hardening practices adopted by Centercode.

3. Web Servers

The Centercode Platform runs on Microsoft Windows 2008 R2 Server, using Microsoft Internet Information Server 7.5 finely tuned and optimized for the Centercode Platform. Web servers are locked down using various security hardening practices adopted by Centercode, and are shielded by strict rules put in place at our firewall.

4. Facility (Rackspace)

The Centercode Platform sits in private locked cages located in a high security facility in Chicago Illinois. Information regarding this facility may be found at www.rackspace.com.

Rackspace maintains a SAS 70 Type II certification. The datacenter is physically manned and monitored 24x7x365, and incorporates best practice security measures such as biometric scanning, video surveillance equipment throughout the facility, and proximity card and identification badge requirements for access to the Datacenter.

5. Network, Server and Application Health Monitoring

The health of every Centercode implementation is automatically monitored. Anomalies are immediately reported to Network Operations and Centercode personnel for appropriate action. This is achieved using a customized **Nagios** server and proprietary profiling tools that were developed by Centercode specifically to monitor the health of the Centercode Platform.

Additionally, each server's individual resources are monitored to ensure we know when such resources are in danger of becoming inadequate for their given activity level.

IV. Standard Practices

The following defines our standard operational practices for maintaining the Centercode application.

1. Data Backup

Database data is backed up locally every 12 hours. Complete backups (files and database) are backed up off site daily. Backups are retained for 4 weeks.

2. Activity Logging

The Centercode application is designed to maintain a record of all activity that occurs within the application. Should a breach be identified either by our own mechanisms (such as our IDS systems), or as reported to us by a customer or user (for example they receive a notification that their personal information has been changed, but did not themselves request the change), we will be able to reconstruct the actions that lead to the event.

Every page load that occurs within the Centercode application is recorded with each user's session, and can be matched with web server logs to provide further detail of the path a user account had followed through the application. Every administrative action is tagged with the date, time and user account that affected a change. Every email message that is sent from the application is tagged and logged within our system.

Historic values are recorded for information that is deemed to be particularly sensitive, such as basic personal account information and Project Feedback information.

3. Scheduled Maintenance

Scheduled maintenance, such as database platform and operating system patch application, is deployed locally in a test environment prior to being introduced to any Centercode production environment. Each patch is tested thoroughly before live deployment.

All data is backed up prior to any major server update, allowing for lossless recovery in the event of any maintenance failure. Customers are notified via email prior to any scheduled maintenance.

4. New Releases

Centercode updates, such as bug fixes and incremental version releases, are pre-scheduled and handled with the same methodologies and timeframes as scheduled maintenance (see above).

5. Regularly Scheduled Vulnerability Scan

We regularly scan our networks to check for:

- Vulnerabilities that allow a remote hacker to control or access sensitive data on a system
- Misconfiguration (e.g. open mail relay, missing patches, etc.)
- Default passwords, a few common passwords, and blank/absent passwords
- Denials of service against the TCP/IP stack by using mangled packets

6. Customer Sponsored Security Audits

We are willing to authorize and make appropriate arrangements for individual customers to test our security infrastructure via their own resources or outsourced security firm. This is a scheduled event, which is designed to take place apart from our primary network — thus not affecting live implementations.