Ministry Mobilizer (version 6.1)

Web Application Security Overview

January 3rd, 2012

Overview 3

Security Assessment 3

Data Safety 3

Data Access Security at Priority's Database Server 4

Web and Database Server Firewalls 4

Codebase Access Safety 5

Data Access Security via Ministry Mobilizer 5

1. Injection 5
2. Cross-Site Scripting (XSS) 5
3. Broken Authentication and Session Management 6
4. Insecure Direct Object References 6
5. Cross-Site Request Forgery (CSRF) 6
6. Security Misconfiguration 7
7. Insecure Cryptographic Storage 7
8. Failure to Restrict URL Access 7
9. Insufficient Transport Layer Protection 7
10. Unvalidated Redirects and Forwards 7

Security in Authentication and Authorization of users for Ministry Mobilizer 8

User Creation and Initialization 8

Security Factors in Authentication 9

Password Strength and Expiration Policy 9

Password Storage 9

Password Retrieval 9

Lockout Policy 9

Authorization 9

Overview

This document serves as a general outline of the security environment that currently exists for Priority Research's (DBA. Protect My Ministry) web application Ministry Mobilizer. The following main sections explain individual security practices in more detail, and describe the specifics of Priority's security for each:

- Data Safety
- Database Server Access Security
- Firewalls
- Codebase Security
- Application Data Access Security
- User Authentication and Authorization Security
- Audit Concerns

Security Assessment

Data Safety

"Data Safety" refers to the security of Priority's data outside of a deliberate hacking attempt: How recoverable the data is from issues like the hardware failure of the server, or any accidental erasures of data that might result from a legitimate operation.

At this time the data safety of the database is managed off-site by Rackspace and then entire state of the server is backed up by Rackspace nightly. Considered a leader in the field of web hosting and data center operations, Rackspace data centers are engineered to the highest levels of reliability, with extensive systems to address security and network redundancy.

Rackspace Physical Security

Keycard protocols, biometric scanning protocols and round-the-clock interior and exterior surveillance monitoring are the basics of Rackspace's physical security. Only authorized data center personnel are granted access credentials to Rackspace data centers; no one else can enter the production area of the datacenter without prior clearance and an appropriate escort.

Rackspace Personnel Vetting

Every Rackspace data center employee undergoes multiple and thorough background security checks before they are hired. Each employee is finger-printed and retina scanned upon hiring; these identifying access credentials are removed from the system in the event of termination or extended leave.

Data Access Security at Priority's Database Server

Priority's production data is stored on a dedicated production SQL Server, running the latest version (SQL Server 2008 R2) with all current patches and security updates applied.

The server is fully dedicated to database operations and is used for no other purpose. It does not host any other applications.

Communication between the database server and the web application server takes place behind the Rackspace firewall. External clients only see data as controlled by Ministry Mobilizer, and the Internal Admin application.

Web and Database Server Firewalls

Most people imagine a "hacker" to be someone that sits in front of a keyboard late at night, guessing passwords to steal confidential data from a computer system. While this type of attack does happen, it makes up a very small portion of the total network attacks that occur. Today, worms and viruses initiate the vast majority of attacks and they generally find their targets randomly. Worms and viruses have dramatically increased the need for network security of all kinds—especially the need for firewalls.

Priority's servers are protected by the following firewalls:

Host-Based Firewall

Host-based firewalls protect an individual computer regardless of the network it's connected to.

Priority's web and database servers use Windows Firewall with Advanced Security to filter two-way network traffic based on specific OAA security protocols which blocks unauthorized network traffic flowing into or out of the OAA server.

Network Firewall

Network firewalls protect the perimeter of a network by watching traffic that enters and leaves.

Priority's web and database servers are guarded by an industrial-strength Cisco PIX hardware firewall, a device designed to prevent unauthorized access to or from a private network. All messages attempting to enter or leave Priority pass through the firewall which examines each message and blocks those that do not meet the firewall's security protocol.

Codebase Access Safety

The entire codebase for Priority is securely stored in an enterprise-class versioning control system (Team Foundation Server) and it is backed up nightly. Only authorized developers can access the code base. No un-compiled source code is deployed to Priority's web servers.

Data Access Security via Ministry Mobilizer

The following section addresses security risks and mitigation approaches within the largest avenue to viewing Priority's data, which is Priority's web applications themselves.

Priority's assessment of security risks and their mitigation follows the Open Web Access Security Project's Top 10 Application Security Risks framework for threat assessment. OWASP is an internationally-recognized non-profit standards group. Their recommendations are adopted worldwide by governmental and private corporations, in addition to certification-granting standards bodies.

The OWASP Top 10 Security Risks, and how Ministry Mobilizer is designed to address them, are summarized as follows:

1. Injection

Injection flaws, such as SQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data.

Mitigation Approach

Ministry Moblilizer uses Entity Framework .NET classes to parameterize all database operations, minimizing the possibility of a SQL injection attack. Entity Framework acts as a middle layer which abstracts the data access from the actual database, so any data commands are to the Entity Framework and not the database. This presents a minimal attack surface.

Furthermore, in Ministry Mobilizer there are no places where input is used to form a dynamic query, so SQL injection of any form simply has no entry point to happen at all.

Ministry Mobilizer does expose some internal data over the querystring as it passes from page to page. If a user attempted to inject by changing these, his next page request would fail unless he entered a legitimate value, in which case it would be no different from a legitimate usage.

2. Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Mitigation Approach

Priority validates all input on the client side before submission to the web server. Additionally because of the use of Entity Framework as described above, there is no real possibility of this kind of attack.

3. Broken Authentication and Session Management

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.

Mitigation Approach

In Ministry Mobilizer, the entire web application is secured using Windows Forms Authentication. Only the login page is presented to an untrusted user, and after that all communication takes place secured over SSL. Sessions are limited in duration to 30 minutes of inactivity.

4. Insecure Direct Object References

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

Mitigation Approach

As mentioned previously, a minimal amount of implementation data is presented to authorized users, and this implementation data is checked during page requests. This data could not be used to mount an injection attack, in any event.

5. Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

Mitigation Approach

Ministry Mobilizer is sandboxed and stand-alone in nature. Authorization is internal to the application and is not be able to grant access to anything other than the pages and data in use by the application. All pages are isolated to a single directory and application pool, and each request is checked to ensure that only data legitimately available to a particular user gets served to that user, preventing the viewing or modification of other users' data at all times.

6. Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. All these settings should be defined, implemented, and maintained as many are not shipped with secure defaults. This includes keeping all software up to date, including all code libraries used by the application.

Mitigation Approach

Priority has built Ministry Mobilizer using the latest Microsoft stack, .NET 4.0 with all relevant patches and security updates applied prior to its production release.

7. Insecure Cryptographic Storage

Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.

Sensitive data in Ministry Mobilizer is protected appropriately.

8. Failure to Restrict URL Access

Many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway.

Mitigation Approach

All of Ministry Mobilizer's assets are contained within a single web application and directory, and access to such assets does not need to be restricted once authorization is granted. Ministry Mobilizer does not contain any interstitial or hidden pages, and does not rely on other sites to display on-page assets.

9. Insufficient Transport Layer Protection

Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly.

Mitigation Approach

All pages are served via SSL.

10. Unvalidated Redirects and Forwards

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

Mitigation Approach

Ministry Mobilizer performs access checking on a per-request basis to ensure that only data and pages which should be viewed by a specific user are being viewed by that user. There is no acceptance of requests from external sites without passing through login authentication, and both authentication and authorization are specific only to Ministry Mobilizer.

There is one instance where Ministry Mobilizer redirects to an external site, and that is when it opens a separate window to our background reports server to view the PDF of a completed background report.

At that point, it is the background reports server which requires security, to ensure that it is validating where the request is coming from. This is a read-only one-way interaction with the background reports server, so there's no possibility of forging a request to reflect back into Ministry Mobilizer at that point.

Security in Authentication and Authorization of users for Ministry Mobilizer

The real protection on the viewing of Ministry Mobilizer data depends in the majority on the security of the doorway into it—how and what the web application itself does to let users through the door. The following points summarize how legitimate users of Ministry Mobilizer are defined and confirmed.

"Authentication" means how the user identity is confirmed, and that trust is established that a user is who they say they are. "Authorization" means how it is determined what a user does or does not get access to within the application.

Generally users are authenticated and then authorized as they proceed through the application. However, you can have one without the other. For instance, everyone is authorized to see the messages that are displayed on Ministry Mobilizer's logon screen—there is no authentication required for that.

User Creation and Initialization

Users are created only by operators, which is technically the highest level of security (as opposed to Ministry Mobilizer allowing users to sign up completely automated and allowing access with no human intervention). However, there are no checks or controls on Priority administrators or administrative client users creating child users.

Security Factors in Authentication

Each user is required to provide a unique username and password to be allowed access to Ministry Mobilizer, for a two-factor authentication scheme.

Password Strength and Expiration Policy

In Ministry Mobilizer there is no expiration policy; a password can last forever. There is no strength policy beyond a minimum length. On login, passwords also do not have case sensitivity—a password given in all-caps is considered the same as one in lowercase.

Password Storage

Passwords are securely stored in the database.

Password Retrieval

There is currently no password retrieval in Ministry Mobilizer other than staff or a parent user manually logging in and finding out what a password is and then telling that to whomever needs to know it. Therefore that piece is as secure as it can be—operator intervention required.

Lockout Policy

Ministry Mobilizer does not have any lockout policy. A user can try infinite times to log in.

Authorization

Ministry Mobilizer authorization generally relies first on the concept of a "Parent User", which is inferred by examining data in a user record (a Parent User is one that has no further parent, and is missing other pieces of data). This causes logic to have to be evaluated on every page to determine whether the current user is a Parent or not to authorize certain actions.