m-Power

mrc

Solving the Top 10 Application Security Threats

Intro

Cyberattacks are increasing, and the problem is only growing worse.

How bad is the problem? The number of U.S. data breaches reached a record high in 2014, with a staggering 43% of companies experiencing a data breach.

How much does a cyberattack cost a company? One study finds that the costs of data breaches has increased 15%--up to $3.5 million. To make matters worse, a publicized security breach causes irreparable damage to a company. It creates negative publicity, damages consumer trust, and leads to angry customers.

*Photo credit: *sax via photopin cc*

The problem: A recent study estimates that 96% of all web applications contain at least one 'serious vulnerability.'

The fact is, hackers have become more advanced. Attacks have become increasingly sophisticated. A data breach creates more damage than ever.

But, web application security isn't keeping pace. Businesses still create insecure applications. Their poor development security practices put their data (and their customer's data) at risk.

Joseph Feiman, lead analyst for application security at Gartner doesn't believe this problem is going away: "Developers will keep developing insecure code, and there's nothing they can do about it. It's a losing battle with hackers."

Why is this happening? Why haven't development efforts kept pace with evolving security risks? Why do developers still create web applications with the same vulnerabilities year after year? Here are a few common reasons:

- **No incentives for security**: Peter Drucker is famously quoted as saying, "What is measured improves." The problem for many developers: Security isn't measured. Developers get recognition for the application features and development speed, not security.

- **New developers in the workforce:** New developers are constantly entering the workforce. They're stuck maintaining code they didn't develop, and don't always understand what a weakness looks like. These new developers make the same security mistakes as their predecessor.

- **Short deadlines harm security**: As businesses place greater importance on application development speed, security suffers. Developers rush through the project—ensuring it meets all the business requirements. But, this often comes at the expense of proper security practices.

- **Businesses treat security like a feature:** Shortly after the healthcare.gov site went live, a "white hat" hacker testified on Capitol Hill that security was never properly built into the site. Many businesses struggle with this same problem. They treat security like any other feature that they can add to an application. The problem: Security isn't something a developer can add at the end. You must build security into the application.

How can you solve the web application security problem?

How can businesses fix this issue? Or, perhaps a better question: Why do so many businesses still struggle with web application security after all of these years?

Image Credit: Helga Weber via photopin cc

Here's one big reason: They try to tackle the security problems on their own. They try to train their developers on all aspects of proper web app security. They try to build all of the security features into their applications. They try to keep up-to-date on all security updates, risks, and new vulnerabilities.

But, what happens when they bring in new developers? What happens when risks change, or new vulnerabilities emerge? What if a developer takes some security shortcuts in an effort to meet a tight deadline?

The problem with security issues: You don't know they're there until it's too late.

How can you develop web applications with the assurance that proper security is built in? How can you keep up with the evolving security risks?

Here's one option: Implement a web application development platform like m-Power.

m-Power is a web application development platform that automates web (and mobile web) application development. It not only lets you develop web applications quickly, it includes the security features you need to protect your business applications from the biggest threats.

m-Power comes with enterprise-class security baked in, and is regularly enhanced with the latest security features. It provides simple, point-and-click options to implement and adjust application security to fit your business.

What security risks does m-Power address?

Proper security protects against external and internal risks. Businesses must protect themselves from external attackers, while controlling internal user and data access. m-Power protects your business on both fronts.

In this paper, we'll explore the biggest security risks facing business applications today, and explain how m-Power protects you from each one. What are these risks? You can find them in the OWASP Top 10 list.

The 10 Biggest Application Security Risks (OWASP Top 10)

The Open Web Application Security Project (OWASP) is a highly-respected online community dedicated to web application security. Their "OWASP Top Ten" list outlines the biggest security vulnerabilities facing modern web applications. Here are the top 10 web application security vulnerabilities, as outlined in the OWASP top 10:

1. Injection

In a code injection attack, attackers insert malicious code into an entry field for execution. SQL injection is the most common injection attack. SQL injection is possible when user input fields allow SQL statements to query the database directly.

Image Credit: PhotoLizM via pixabay cc

Problems created by this risk

SQL injection attacks can ruin a database. Using SQL injection, an attacker can:

- spoof identity,
- tamper with existing data,
- void transactions,
- change account balances,
- allow the complete disclosure of all data on the system,
- destroy the data or make it otherwise unavailable, and
- become administrators of the database server.

How m-Power addresses this vulnerability

m-Power applications include many built-in features to protect against injection attacks. Here are a few examples:

1. **Validated input**
   m-Power validates user input by default, using basic edit checking. This ensures that the content entered via the UI is appropriate for each field.
2. **White-lists and black-lists**
   m-Power lets you add configurable white-lists and black-lists to your applications. These can further restrict user input, and prevent applications from processing malicious character combinations.
3. **Bind Variables**
   m-Power takes advantage of bind variables (parametrized queries) when running SQL queries. Bind variables reduce the risk of injection when constructing queries that include user input.

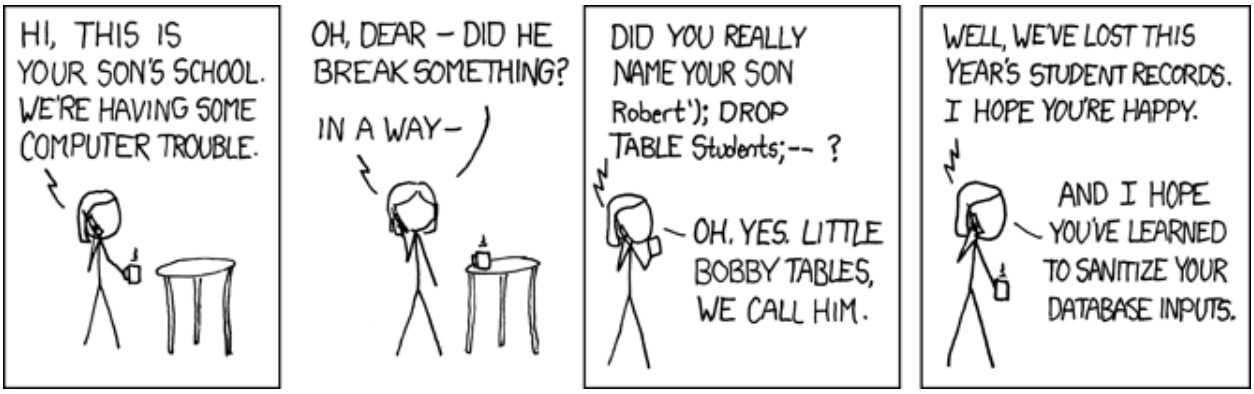

Image Credit: XKCD, "Exploits of a Mom", cc

2. Broken authentication and session management

This security risk stems from improper implementation of authentication and session management function. It lets attackers assume user identities and perform any action that user could perform. Privileged accounts are frequent targets of this attack.

Problems caused by this risk

This vulnerability gives attackers full access to a user's account, or all accounts in a system. Once the attacker gains access, they can do anything the victim could do, such as:

- place orders,
- alter data,
- add/remove data,
- and more.

How m-Power addresses this vulnerability

m-Power lets you configure authentication to store encrypted passwords using various hash functions. m-Power can then perform authentication against the encrypted passwords.

3. Cross-Site scripting

Cross-site scripting (XSS) lets attackers inject client-side script into Web pages viewed by other users. An XSS vulnerability arises when Web applications take data from users and dynamically include it in Web pages without first properly validating the data.

Problems caused by this risk

With XSS, an attacker can perform malicious actions, such as:

- take over a user account,
- spread viruses,
- remotely control the user's browser,
- scan /exploit intranet appliances and applications,
- and more.

How m-Power addresses this vulnerability

m-Power protects against XSS in a couple of ways. First, m-Power applications HTML encode all values returned to the screen that may include user supplied values. Second, m-Power provides you with configurable white-lists and black-lists. This lets you restrict user-supplied input to only allow suitable content. m-Power can scrub unnecessary content and characters before rendering content back on the screen.

4. Insecure Direct Object References

This risk occurs when a developer exposes a reference to an internal implementation object in the URL string. When a file, directory, database key or internal ID number is visible in a URL, your data is at risk. Hackers can manipulate vulnerability to gain access to your users' sensitive data.

Image Credit: mkweb2 via pixabay cc

Problems caused by this risk

With this vulnerability, an attacker could access and manipulate your organization's data. For instance, they could:

- access customer account information,
- charge online purchases to user's credit cards,
- leak sensitive corporate data,
- and more.

How m-Power addresses this vulnerability

m-Power lets you restrict access to internal resources via various application server configuration settings. You can also customize error messages to ensure that information about internal resources is not visible to end users in the event of an error.

5. Security Misconfiguration

Modern web applications have many layers, each needing their own security. You must secure the application, frameworks, application server, web server, database server, and platform. If each layer is not properly configured, it opens the door to an attacker.

Problems caused by this risk

Faulty security configurations let attackers compromise a system unnoticed. They can steal or modify data slowly over time--which can be time-consuming and expensive to recover.

How m-Power addresses this vulnerability

mrc updates frameworks used on a regular basis and expedites patches for known issues. Default users and passwords for application server management are also configurable by m-Power administrators.

6. Sensitive Data Exposure

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

Image Credit: carlosalbertoteixeira via pixabay cc

Problems caused by this risk

Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. A sensitive data breach not only gives your company a bad name, but also puts your business at risk of lawsuits from victims of the data breach.

How m-Power addresses this vulnerability

m-Power lets you encrypt any value deemed necessary using encryption objects. These objects support multiple levels of encryption as needed. They can encrypt values such as credit cards, passwords, and other types of sensitive data prior to storage in a database.

7. Missing Function Level Access Control

Web application functions are the capabilities of an application. Access controls limit the web application functions based on user privileges. When web applications lack these access controls, they open the door for a data breach.

Problems caused by this risk

These flaws allow unauthorized user access. It can give internal/external users administrative access to your applications. This vulnerability can lead to compromised systems and data loss.

How m-Power addresses this vulnerability

m-Power offers two options to protect against this threat:

- **Role based application level access control**: This security feature lets you limit application and data access based on user or role. Users will only see the data or applications they're authorized to see.
- **Feature based "User Privilege" access**: This security feature lets you control application features on a per-user basis. This ensures that only appropriate users can access any particular function within m-Power web applications.

8. Cross-Site Request Forgery (CSRF)

A CSRF attack occurs when a malicious website sends a request to a web application that a user is already authenticated against from a different website. The attacker can force the victim's browser to generate requests. Applications not protected from a CSRF attack think these requests are legitimate requests from the victim.

Problems caused by this risk

Attackers can trick victims into performing any state changing operation the victim can perform. For example, an attacker could:

- update the user's account details,
- make purchases,
- logout and login,
- and more.

How m-Power addresses this vulnerability

m-Power applications lets developers enable CSRF tokens in forms that perform sensitive actions. Developers can choose to enable this level of protection when necessary. Enabling CSRF tokens can ensure that a cross-site request forgery fails to manipulate an action as a logged in user.

9. Using components with known vulnerabilities

Most software today uses external components, frameworks, or libraries. These components often run with full privileges. If just one of those components contains a known vulnerability, it is a prime target for an attacker. A single vulnerability can compromise an entire system.

Image Credit: 44833 via pixabay cc

Problems caused by this risk

This vulnerability opens the door to injection, broken access control, XSS, etc. The impact could range from partial to complete system and data compromise.

How m-Power addresses this vulnerability

mrc patches and keeps its libraries and frameworks up to date. This mitigates the possibility of attacks via known vulnerabilities.

10. Unvalidated redirects and forwards

Some web applications redirect users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to unsafe sites, or use forwards to access unauthorized pages.

Problems caused by this risk

With this vulnerability, an attacker may infect users with malware, or launch a phishing scam and steal user credentials. This can lead to compromised applications and systems, giving an attacker full access to your data.

How m-Power addresses this vulnerability

m-Power provides configurations that let developers restrict redirects to specific applications. In the event that a redirect appears configurable by an end user, these configurations ensure that the server will only allow a redirect to a predefined set of applications.

Summary

Despite the rising importance of proper security, best practices are often ignored. Basic security mistakes still plague many web applications.

As more development shifts to the web, and more data is stored on the cloud, security is a critically important topic. A single security misstep can compromise confidential business data or your customer's personal information. It can lead to millions of dollars of losses, and cause irreparable damage to your company.

What web application security risks must businesses protect themselves against? The OWASP Top Ten lists these as the biggest web application security risks facing businesses today:

1. Injection
2. Broken Authentication and Session Management
3. Cross-site Scripting (XSS)
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross-Site Request Forgery (CSRF)
9. Using Components with Known Vulnerabilities
10. Unvalidated Redirects and Forwards

How can businesses better protect themselves from these security risks?

Use an application development platform like m-Power.

m-Power lets anyone in your company develop secure web applications without coding. It includes the tools you need to protect your web applications from the biggest application security risks facing businesses today.

With m-Power, you don't need to worry about creating security measures from scratch. You don't need to wonder how you'll address every security risk. m-Power offers powerful security features and configurations that you can implement and adjust to meet your needs.

To learn more about m-Power, visit our website at http://www.mrc-productivity.com.