HOW TO WRITE SECURE WEB APPLICATIONS – FROM ZERO TO HERO

BY STEPHEN WOMACK

AGENDA

- Where we are today
- Principles to follow
- Resources
- Q & A

WHERE WE ARE IN WEB APP SECURITY

TARGET SECURITY BREACH

"… reporting a range of 70 million to 110 million people." – New York Times

ANTHEM SECURITY BREACH

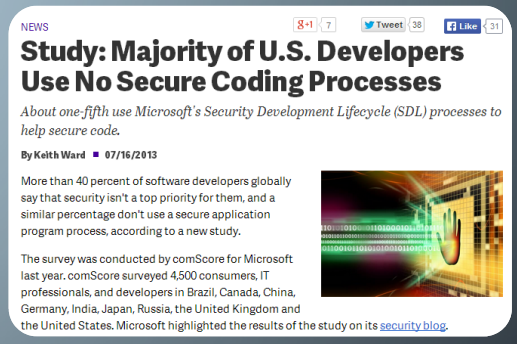
"In all, Anthem said the compromised database included 80 million records related to current and former customers and employees." – arsTechnica

“AS MANY AS 1 MILLION+ WORDPRESS SITES IMPERILED BY CRITICAL PLUGIN BUG”

"Successful exploitation of this bug could lead to Blind SQL Injection attacks, which means an attacker could grab sensitive information from your database, including username, (hashed) passwords and, in certain configurations, WordPress Secret Keys (which could result in a total site takeover)."

MAJORITY OF U.S. DEVELOPERS USE NO SECURE CODING PROCESSES – VISUAL STUDIO MAGAZINE

"More than 40 percent of software developers globally say that security isn't a top priority for them, and a similar percentage don't use a secure application program process, according to a new study."



NEWS

Study: Majority of U.S. Developers Use No Secure Coding Processes

About one-fifth use Microsoft's Security Development Lifecycle (SDL) processes to help secure code.

By Keith Ward ■ 07/16/2013

More than 40 percent of software developers globally say that security isn't a top priority for them, and a similar percentage don't use a secure application program process, according to a new study.

The survey was conducted by comScore for Microsoft last year. comScore surveyed 4,500 consumers, IT professionals, and developers in Brazil, Canada, China, Germany, India, Japan, Russia, the United Kingdom and the United States. Microsoft highlighted the results of the study on its security blog.

MAJORITY OF U.S. DEVELOPERS USE NO SECURE CODING PROCESSES – VISUAL STUDIO MAGAZINE

"Comparatively, a staggering 76 percent of U.S. developers use no secure application program process …"

"The only country with a higher percentage was Japan, which ended up at the very end of nearly every category, at 80 percent."

"NASDAQ IS OWNED." FIVE MEN CHARGED IN LARGEST FINANCIAL HACK EVER

"… exploited SQL-injection vulnerabilities in the victim companies' websites to obtain login credentials and other sensitive data"

"… he said, '30 SQL servers, and we can run whatever on them, already cracked admin PWS but the network not viewable yet. those dbs are hell big and I think most of info is trading histories.' "

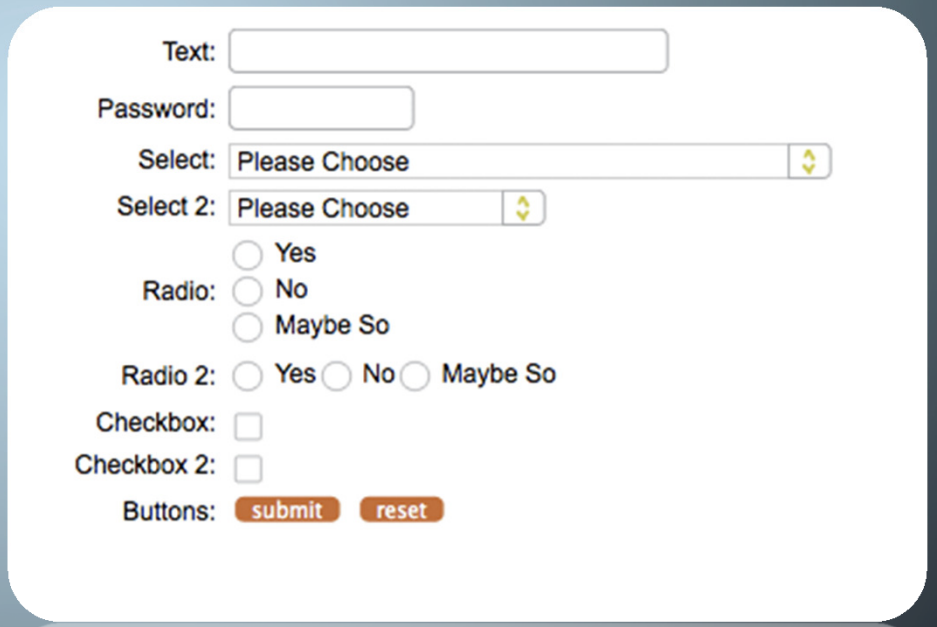
5 PRINCIPLES FOR SECURE WEB APPS

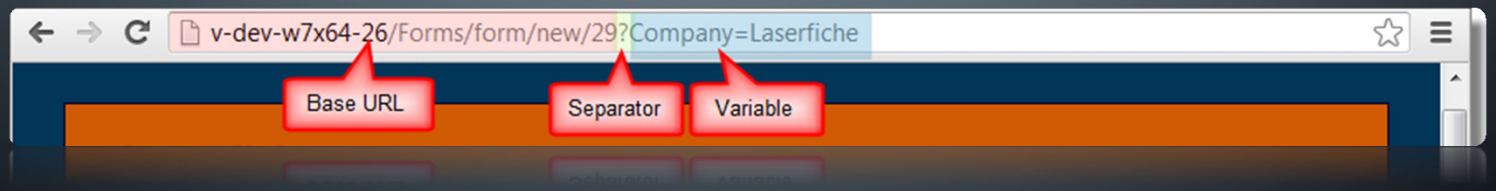

www.toddconner.net


1. DO NOT TRUST ANYONE
USER INPUT OR SERVICE CALLS

VALIDATE ALL INPUT

- Length of text
- Validate drop menu selection
- Validate proper characters like numbers and dates
- Use RegEx to White List characters





Example:

http://localhost/wordpress/index.php?paged=-1

Result:

WordPress database error: [Erreur de syntaxe pr?s de '-20, 10' ? la ligne 1]
SELECT DISTINCT * FROM wp_posts WHERE 1=1 AND post_date_gmt <= '2006-06-29 12:46:59' AND (post_status = "publish") AND post_status != "attachment" GROUP BY wp_posts.ID ORDER BY post_date DESC LIMIT -20, 10

~ Full path ~

/wp-settings.php
/wp-admin/admin-footer.php
/wp-admin/admin-functions.php
/wp-admin/edit-form.php
/wp-admin/edit-form-advanced.php
/wp-admin/edit-form-comment.php
/wp-admin/edit-link-form.php
/wp-admin/edit-page-form.php

USE BEST PRACTICES

- OWASP best practices
- Microsoft best practices
- Your team's coding standards
  - If you do not have a standard, create one!

PREVENT CROSS SITE SCRIPTING

FOLLOW THE RULE OF LEAST PRIVILEGE

- Show users only what information they need
- Use roles and permissions to control what is seen

```
[AllowAnonymous]
public ActionResult Index()
{
    return View(db.Comments.ToList());
}
```

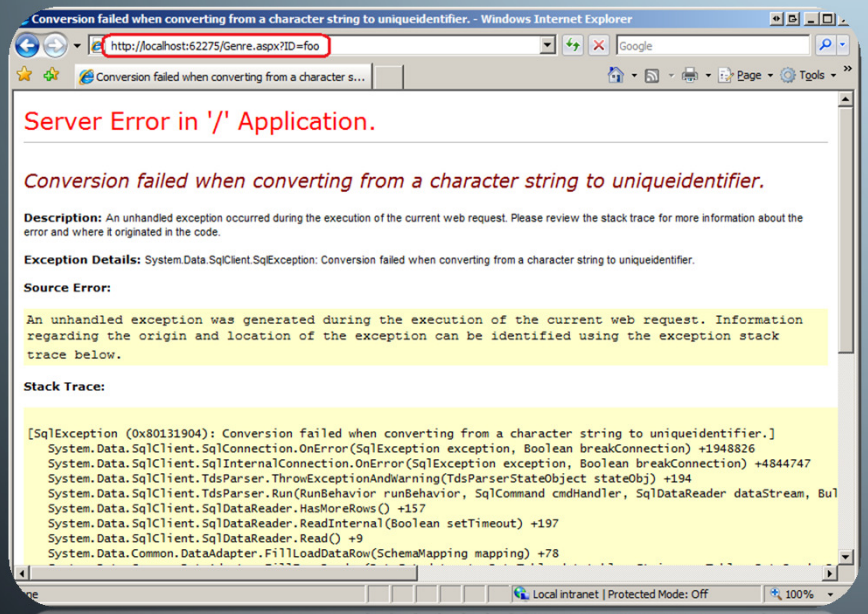
2. FAIL SECURELY

HANDLING ERRORS PROPERLY IS AN IMPORTANT PART OF SECURE CODING

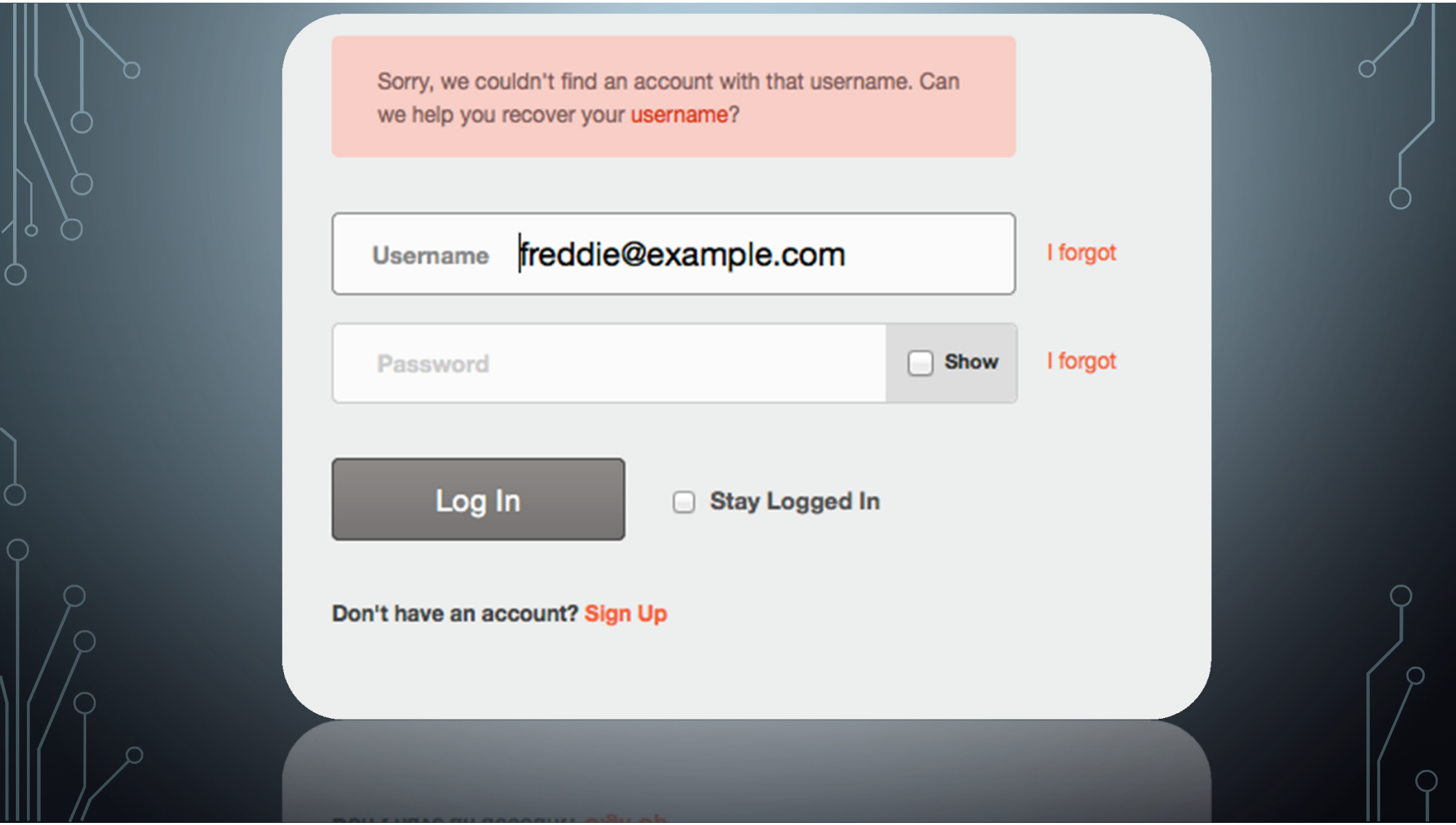
YOUR CODE SHOULD BE DESIGNED IN SUCH A WAY THAT A FAILURE WILL RESULT IN THE SAME PATH AS DISALLOWING THE OPERATION.

```
public bool IsAdmin()
{
    bool isAdmin = true;

    try
    {
        CodeWhichMightFail();
        isAdmin = IsUserInRole(UserRoles.Administrator);
    }
    catch (Exception e)
    {
        // Logging done here
    }

    return isAdmin;
}
```

DO NOT GIVE OUT TOO MUCH DETAIL




```
<system.web>
    <customErrors defaultRedirect="GenericError.htm" mode="RemoteOnly">
    <error statusCode="500" redirect="~/Error/InternalError" />
    <error statusCode="404" redirect="~/Error/PageNotFound" />
  </customErrors>
</system.web>
```


Sorry, we couldn't find an account with that username. Can we help you recover your username?
Username
freddie@example.com
I forgot
Password
Show
I forgot
Log In
Stay Logged In
Don't have an account? Sign Up


3. CODE REVIEWS
JUST DO IT

“

EVERY MAN IS MY TEACHER, BECAUSE EVERY MAN KNOWS SOMETHING I DON’T KNOW.

”

Jack Hyles

CODE REVIEWS

- People learn from other developers
  - Points out vulnerable code.
  - Shows how to write solid code.
- People catch security mistakes

"**You are not your job.** You are not how much money you have in the bank. You are not the shoes you wear. You are not the contents of your wallet." – fight club

4. ESTABLISH SECURE DEFAULTS

DEFAULT SECURITY OPTIONS TO "ON" - MAKE USERS TURN THEM OFF.

ESTABLISH SECURE DEFAULTS

The experience for the user should be secure by default. It should be up to the user to reduce the security.

- Social Network Privacy Settings
- Remember Password
- SSL

5. TAKE RESPONSIBILITY

“

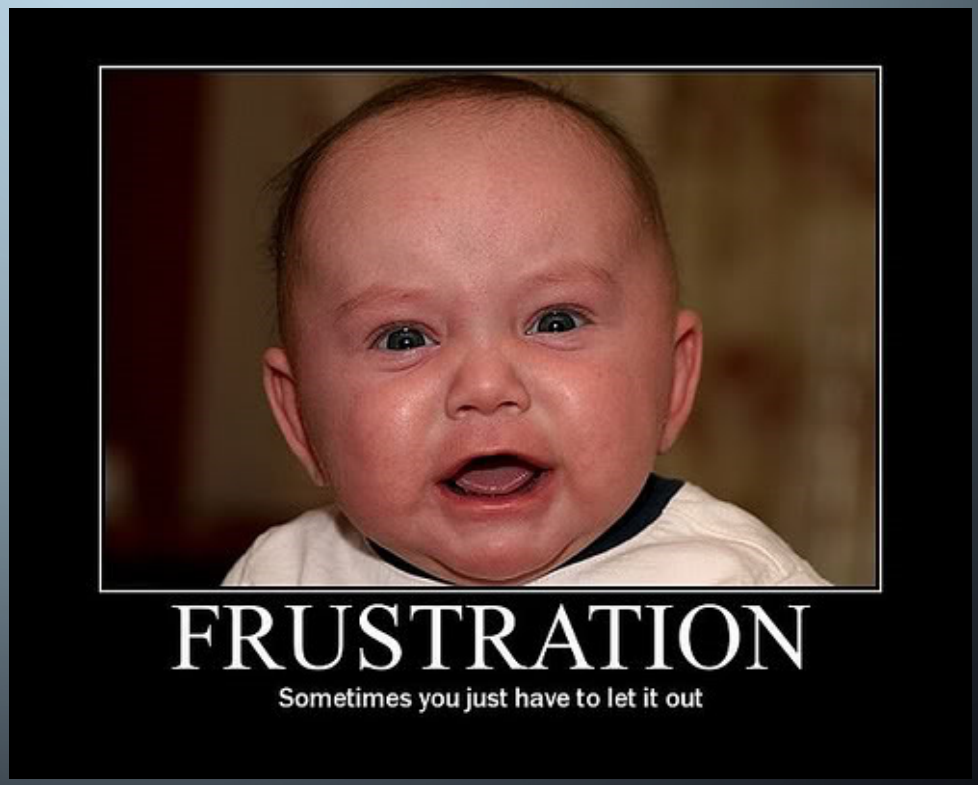
THE PRICE OF GREATNESS IS RESPONSIBILITY

”

Winston Churchhill

IT IS NOT EVERYONE ELSE'S JOB

- Database administrator
- System administrator
- Senior programmer



“

NOT ALL READERS ARE LEADERS, BUT ALL LEADERS ARE READERS.

”

Harry S Truman

READ BOOKS AND ARTICLES ABOUT SECURITY

- Books
  - **24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them by Michael Howard, David LeBlanc, and John Viega**
  - **Software Security: Building Security In by Gary McGraw**
- Websites
  - OWASP top 10 list
  - Security Dark Reading
  - Visual Studio Magazine
  - Defend Your Code with Top Ten Security Tips Every Developer Must Know

KNOW AND USE YOUR TOOLS

- Frameworks
- Libraries

RESOURCES

- OWASP
- Dark Reading
- Microsoft Security Bulletin
- Visual Studio Magazine
- arsTechnica
- Defend Your Code with Top Ten Security Tips Every Developer Must Know

QUESTIONS AND ANSWERS

THANK YOU!

Twitter: stephen_womack

Email: swomack@gmail.com

Presentation: github.com/stephenwomack/SecureWebApps

SOURCE

- http://www.youtube.com/watch?v=jtJ2RyjRqWI
- http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0
- http://visualstudiomagazine.com/articles/2013/07/16/majority-of-us-devs-dont-practice-secure-coding.aspx
- http://arstechnica.com/security/2013/07/nasdaq-is-owned-five-men-charged-in-largest-financial-hack-ever/
- https://www.owasp.org/index.php/Establish_secure_defaults
- http://www.securityfocus.com/archive/1/archive/1/438942/100/0/threaded