Kevin A. McGrail
kmcgrail@InfraShield.com

INFRASHIELD

GDG

A GDE's Guide to Secure Programming

Introduction

IT'S DANGEROUS TO GO ALONE!
TAKE THIS.

Google G Suite TC, GDE & Ambassador

https://www.linkedin.com/in/kmcgrail

INFRASHIELD

Security Expertise

Apache SpamAssassin

KAM.cf

Helped with the first IDS

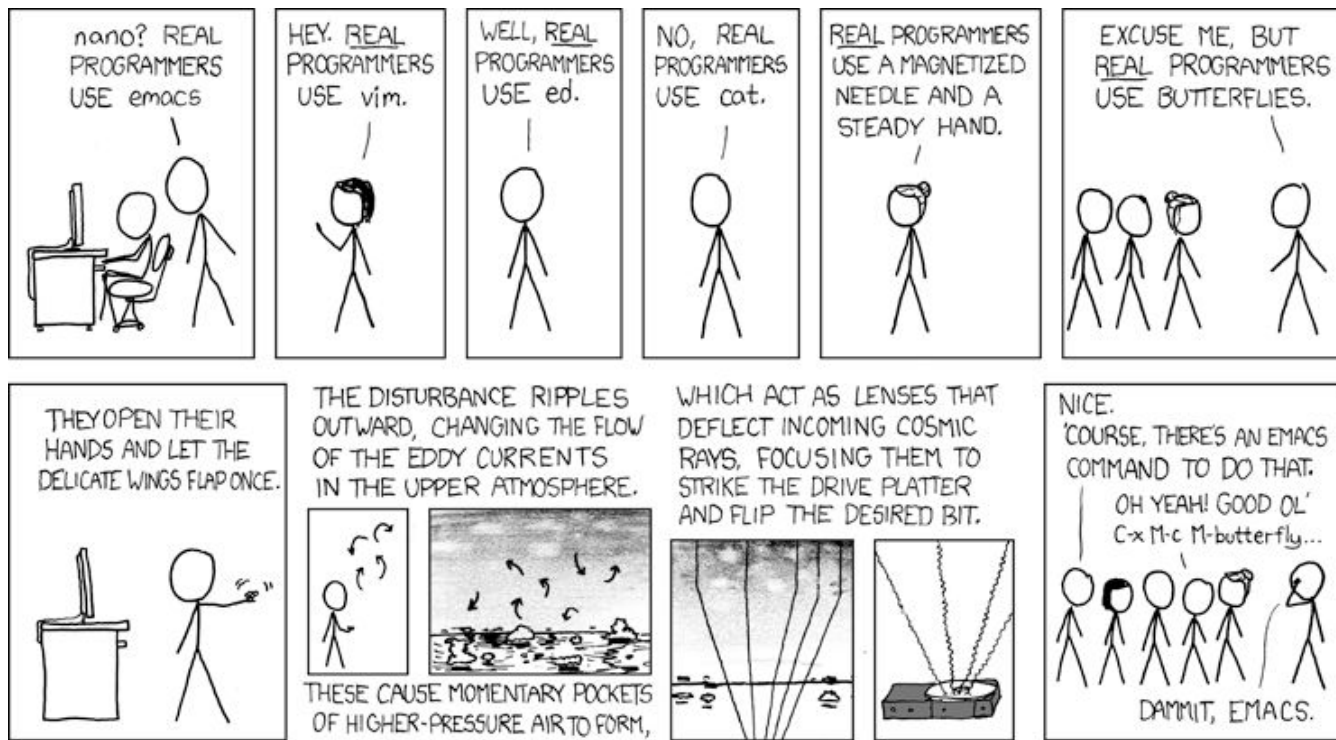MIMEDefang

Phone Lines Cut

Apology letter from the FBI

Google Developers Experts

Seeking? / Hiring?

Tone Setters

xkcd is a source of great knowledge and humor

Rules of Engagement or ROE

Pay attention to your Rules of Engagement

When doing secure programming and secure assessments do NOT breach your ROE

What makes a high-end, security programmer?

- Documents concerns

- Thinks Evil

- Prove if you are wrong or right (follow your ROE)

- Ethically disclose issues

Think Evil

Start with Why:

Threat Modelling is important.

MITRE ATT&CK to understand your adversaries and their TTP (Tactics, Techniques & Procedures)

Palo Alto Networks Unit 42 Playbooks

OWASP Secure Coding Checklist - 10 pages
https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v2.pdf

Payment Card Industry Data Security Specification (PCI-DSS) - SAQ

CIA Triad

Confidentiality, Integrity and Availability

"The only secure computer is one that's unplugged, locked in a safe, and buried 20 feet under the ground in a secret location... and I'm not even too sure about that one."
Dennis Hughes, FBI.

Handling Passwords

Get rid of password complexity and instead use length

National Institute of Standards and Technology (NIST) Digital Identity Guidelines, SP 800-63B Section 5.1.1.2 paragraph 9, "recommends against the use of composition rules (e.g., requiring lower-case, upper-case, digits, and/or special characters) for memorized secrets. These rules provide less benefit than might be expected…"

Support LONG passwords

Passphrases not passwords - xkcd Password Generator & Crypt:HSXKPasswd
https://metacpan.org/pod/Crypt::HSXKPasswd

Don't require periodic password changes

"Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.", SP 800-63B Section 5.1.1.2 paragraph 9

Hashing AND Salting - haveibeenpwned.com

Handling Logins

Support Multi-Factor Authentication (MFA)

NOTE: Google Authenticator is free and
https://metacpan.org/pod/Auth::GoogleAuth

Password Reset capabilities are a key attack. Reset emails, should be single use and short lifespan.

Notify users such as by email when a password is updated/reset.

What is the name of the First all-electronic Computer?

Quiz Break

A: ENIAC

(Electronic Numerical

Integrator And Computer)

KAM's Dirty Dozen

KAM's Top Problems - #1 Security First

Software Development Lifecycle (SDLC)

● Gather the requirements

● Build Security and Privacy in the design - "baked-in, not bolted-on"

● Think Evil at every scrum - Scrum in 2 minutes
  https://www.youtube.com/watch?v=Qoa5CS9JJPQ

● Use test-driven development and include the security requirements

● Use Pen Testing Validation (USAF Fast Track) and Bug Bounty programs

KAM's Top Problems - #2 Input Validation

NEVER TRUST User Data - Input Validation is key

QA Tips:

#1 - If you use client side validation, consider that UX Improvement Only.
    Do all input validation server-side! Assume the front-end is compromised.

#2 - Learn Regular Expressions (man perlre or https://perldoc.perl.org/perlre.html)
    For example, expecting a number? $id =~ s/[^0-9]//g;

#3 - Sanitize user input before it creeps into any dynamic functionality.

KAM's Top Problems - #3 SQL Placeholders

Use SQL Placeholders aka bind values aka parameter markers

```
$query = "SELECT * FROM sessions WHERE user_id = ? AND session_id =
? AND last_password_entry > DATE_SUB(NOW(), INTERVAL 1 HOUR)";
```

QA Thoughts:

#1 Grep your SQL Queries for variables

~~$query = "SELECT * FROM sessions WHERE user_id = $id";~~

#2 Try input variables with single quotation marks and tick marks.

Comic courtesy of xkcd: https://xkcd.com/327/
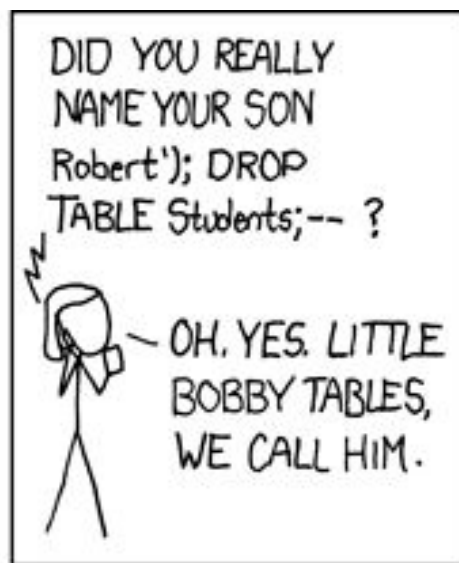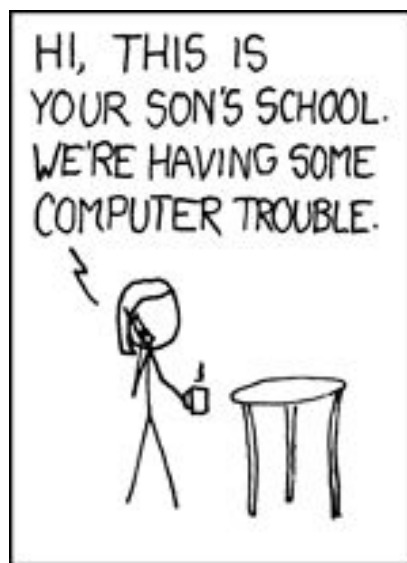
mySQL Example at https://www.techiediaries.com/php-angular/ worries me a little:

```
$id = ($_GET['id'] !== null && (int)$_GET['id'] > 0)?
mysqli_real_escape_string($con, (int)$_GET['id']) : false;

$sql = "DELETE FROM `policies` WHERE `id` ='{$id}' LIMIT 1";

mysqli_query($con, $sql);
```

https://websitebeaver.com/prepared-statements-in-php-mysqli-to-prevent-sql-injection

```
$statement = $mysqli->prepare("DELETE FROM policies WHERE id = ?");

$stmt->bind_param("i", $_GET['id']);
```

KAM's Top Problem #4 - Errors are too informative

Error handling should not disclose too much information.

Provide a tracking number and nothing else.

Log, log, log.

KAM's Top Problems #5 - Improve your Logging

Make sure logging does not include passwords or sensitive material

Restrict log access

Log validation errors in login, and input validation. They can show signs of attackers testing weaknesses.

Look at consolidating logs (syslog, SIEMs, Elastic Search…)

KAM's Top Problems #6 - Use Autonomous Blocks

Use tools like fail2ban to easily add automatic blocks from your logs

Brute Force password attempt blocking should be built-in (be careful of DOSses to lock out the admins)

Consider rate-limiting and blocks per IP address, for example.

KAM's Top Problems #7 - Failing POLP

Use Principles of Least Privilege (POLP)

Do this when developing your code NOT AFTER
Mistakes I've made:

Turning off SELINUX
Grant ALL on Databases
Using elevated privileges for general work as laziness

When elevated privileges are needed, use as short a window as possible!

KAM's Top Problems #8 - Have an Incident Plan

Speed matters!

"Don't Panic"

KAM's Top Problems #9 - No Moral Compass

USENIX / Systems Administrators' Code of Ethics

https://www.usenix.org/system-administrators-code-ethics

Q/EH® Qualified/ Ethical Hacker

CEH Certified Ethical Hacker

KAM's Top Problems #10 - Not Tracking CVEs/News

June 6, 2019:

https://news.cpanel.com/urgent-updates-for-70-76-and-78-and-exim-cve-2019-10149/

& May 28, 2020:

https://www.wired.com/story/nsa-sandworm-exim-mail-server-warning

NOTE: NVD & CVEs can be a sign of MORE secure code because it means the developers are paying attention.

KAM's Top Problems #11 - Dev to QA to Prod

Have a process for code going from dev to QA to production

Automate what you can!

If I gave you a bug fix, how long to release?

KAM's Top Problems #12 - FORKING

212

The # of days I just made up for how long it takes your programmers to backport or forward port changes to a library.

DO NOT FORK

KEEP YOUR LIBRARIES UP TO DATE

KAM's Top Problems #13 - Stupid Mistakes

Always use peer reviews

Pair Programming is Awesome - One person writes, another commits/accepts PR

Jabber with waterfowl?

Return vs Enter

Talk to Your Duck

Seriously?!?

Six Do NOTs

To Quack or Not to Quack
Next Step: XP Pair Programming

Homework

Watch The I.T. Crowd on Netflix Season 3, Episode 4: "The Speech", someone please 3D print me my own internet.

Thanks!

Slides will be on my LinkedIn & mcgrail.com/downloads

Thanks to "The Pragmatic Programmer" where I learned about talking to a duck.

Image Credits:

    KAM photo taken by Ted King, used with permission.

    xkcd Comic https://xkcd.com/378/ & https://xkcd.com/327/ (CC BY-NC 2.5)

    Thanks to James Thompson at cPanel for the Apache SpamAssassin Logo

    Keep Calm Poster from the Public Domain

    Linux Duck - DevRant: https://swag.devrant.com/products/devducks-linux-rubber-duck

    Circle/Slash graphic - Thanks to Pixabay: https://pixabay.com/vectors/red-circle-backslash-no-symbol-24018/

    Ernie & Rubber Ducky - Sesame Place: https://shop.sesameplace.com/products/ernie-and-duck-water-buddy-set

    What the Duck? - Best Cool Gifts: https://www.amazon.com/Funny-Novelty-Gift-Rubber-Best/dp/B07G8GDT8L

    Shakespeare Duck - Samuel White: https://www.pinterest.com/samsmama21/rubber-ducks/

INFRASHIELD

Kevin A. McGrail

www.linkedin.com/in/kmcgrail