Kevin A. McGrail
kmcgrail@InfraShield.com

INFRASHIELD

A Cyber Security Expert's Guide to Secure Programming

Introduction

MAPLE LEAF
READY TO EAT · PRÊT À MANGER
KAM
LUNCHEON MEAT / PAIN DE VIANDE
455
TENEUR ÉLEVÉE EN PROTÉINES
340 g
SUGGESTED SERVING
PRÉSENTATION SUGGÉRÉE

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

INFRASHIELD

Security Expertise

Apache SpamAssassin

KAM.cf

Helped with the first IDS

MIMEDefang

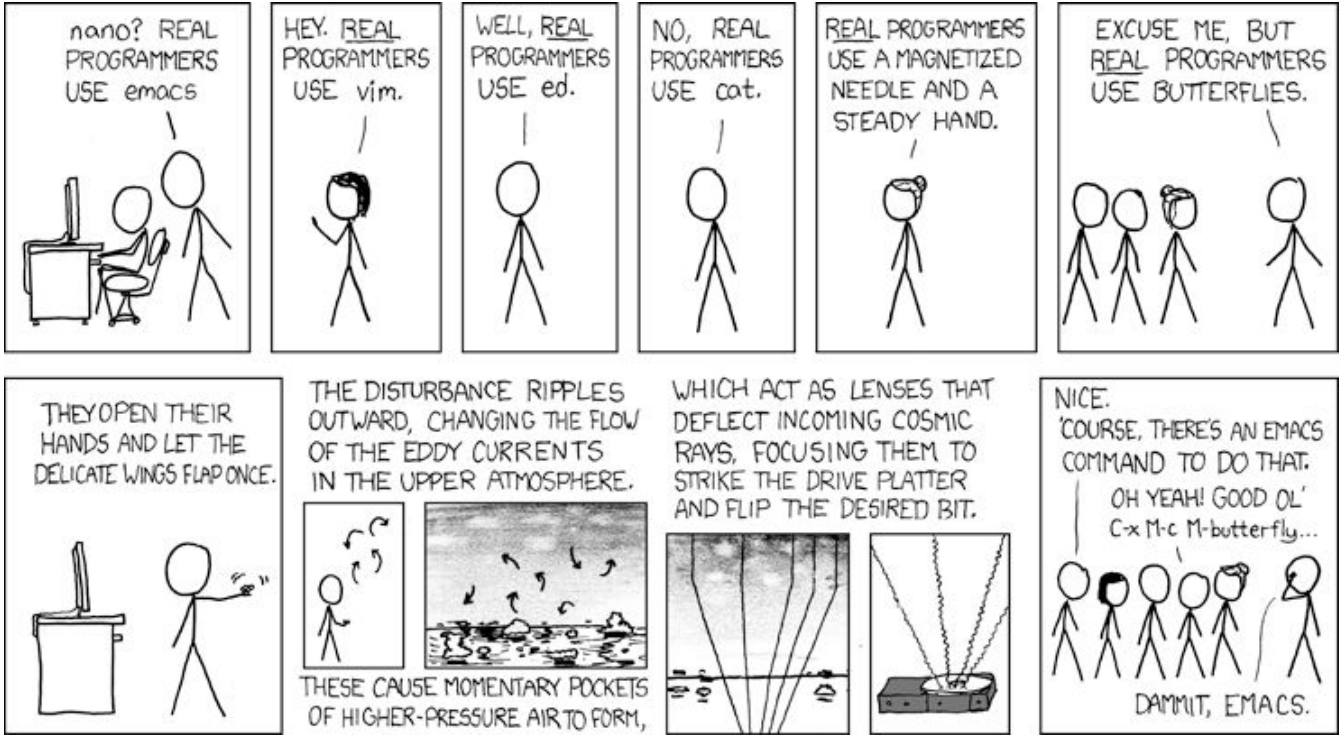
Phone Lines Cut

Apology letter from the FBI

9
THUNDERBIRD

Tone Setters

xkcd is a source of great knowledge and humor


nano? REAL PROGRAMMERS USE emacs
HEY. REAL PROGRAMMERS USE vim.
WELL, REAL PROGRAMMERS USE ed.
NO, REAL PROGRAMMERS USE cat.
REAL PROGRAMMERS USE A MAGNETIZED NEEDLE AND A STEADY HAND.
EXCUSE ME, BUT REAL PROGRAMMERS USE BUTTERFLIES.
THEY OPEN THEIR HANDS AND LET THE DELICATE WINGS FLAP ONCE.
THE DISTURBANCE RIPPLES OUTWARD, CHANGING THE FLOW OF THE EDDY CURRENTS IN THE UPPER ATMOSPHERE.
THESE CAUSE MOMENTARY POCKETS OF HIGHER-PRESSURE AIR TO FORM,
WHICH ACT AS LENSES THAT DEFLECT INCOMING COSMIC RAYS, FOCUSING THEM TO STRIKE THE DRIVE PLATTER AND FLIP THE DESIRED BIT.
NICE.
'COURSE, THERE'S AN EMACS COMMAND TO DO THAT.
OH YEAH! GOOD OL' C-x M-c M-butterfly...
DAMMIT, EMACS.

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.

Quiz Break

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!

#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.

Commercial Break

Use Libraries for Input Validation.

For email addresses, look at Net::validMX https://metacpan.org/pod/Net::validMX

Just released version v2.5.0!

Has been used for a long time in production testing trillions of addresses

KAM’s Top Problems - #3 SQL Placeholders

Use SQL Placeholders aka bind values aka parameter markers

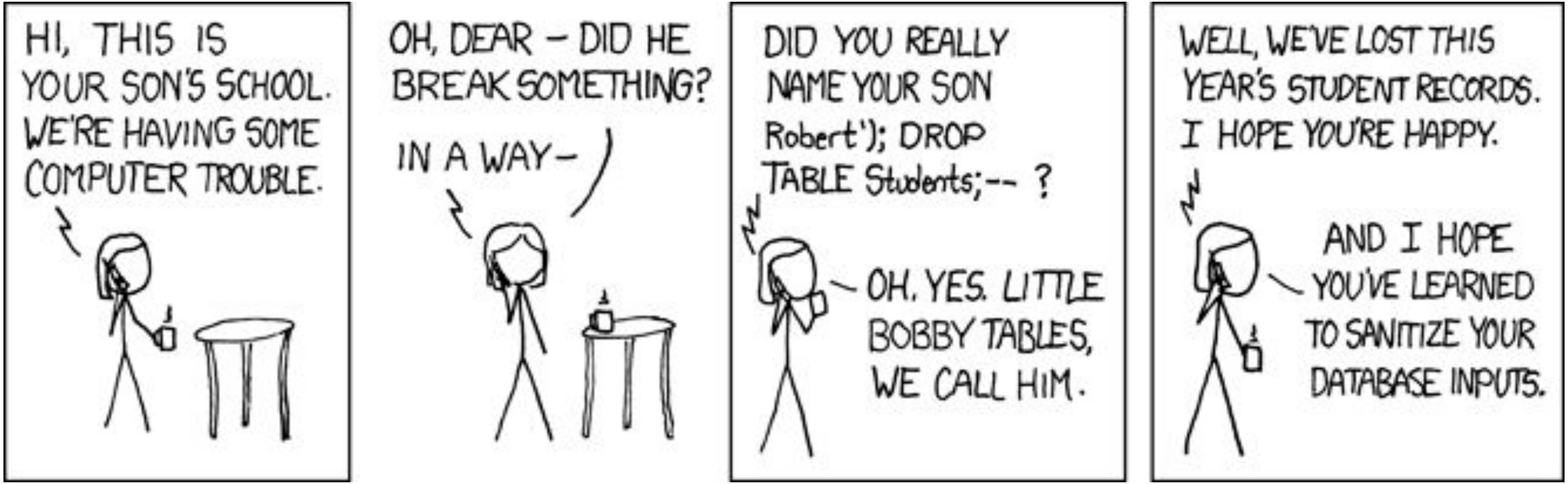
```
$query = "SELECT * FROM sessions WHERE user_id = ? AND session_id = ? AND last_password_entry > DATE_SUB(NOW(), INTERVAL 1 HOUR)";
```

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.


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Comic courtesy of xkcd: https://xkcd.com/327/

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

usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

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 - Stupid Mistakes

Pair Programming is Awesome

Always use peer reviews

One person writes, another commits/accepts PR

Talk to the duck! (Plug: My Lightning Talk will be on Talk to the Duck)

Kevin A. McGrail
kmcgrail@InfraShield.com

INFRASHIELD

Talk to Your Duck
A Lightning Talk
by KAM

Homework

Watch The I.T. Crowd on Netflix

Thanks!

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

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

INFRASHIELD

Kevin A. McGrail
www.linkedin.com/in/kmcgrail