OWASP
Open Web Application Security Project

Defensive Coding

Archzilon Eshun-Davies
CISO/CEO
Tactical Intelligence Security(TAISE)

What am talking about is

These libraries are not secure

1. Only 86% of reported open source security vulnerabilities are included in the CVE database.
2. Your development time does not include security
3. Management knows no libraries, everything is **YOUR** fault.

Be Paranoid

- Turn off error reporting in production (have a config file that does it)
- Log errors to file
- Don’t display user input without formating
- Don’t trust the user
- Don’t mix server side code and UI
- Don’t use alert(...)
- Always check session on pages that require them
- Don’t assume input is always in the correct format
- Check input in the frontend and the backend
- Be sure the DB is returning only what you asked for.

Be Paranoid Contd...

- Escape everything
- Don’t secure only the front door
- Hash your passwords(with a strong crypto)
- Check your logic
- API endpoints can be cracked too
- Implement rate limiting on your API
- Use endpoint security
- etc...

All languages are the same

Don’t assume a language is superior and can survive any attack.

Understand that promises would not always be fulfilled.

Object Oriented is the same everywhere

Read your code again.

RTFM

Read the OWASP “Application Security Verification Standard 3.0” see ref 2

Read the “OWASP Secure Coding Practices - Quick Reference Guide” see ref 3

References

1. https://www.whitesourcesoftware.com/open-source-vulnerability-management-report/#hero_section
2. https://www.owasp.org/images/6/67/OWASPApplicationSecurityVerificationStandard3.0.pdf
3. http://www.owasp.org/images/2/2f/OWASP_SCP_Quick_Reference_Guide_v1-1b.pdf