Security Interventions: Pushing Programmers To Become The Solution

Lloyd Hilsgen

2022

Table Of Contents

Vulnerabilities

What is a vulnerability?

Code vulnerabilities are flaws in code that create a potential risk of compromising security

Vulnerabilities

Why care about vulnerabilities?

Data Breaches:

- 7.9 billion records obtained in data breaches in 2019 [3]
- The average cost per US record stolen is $164 [1]
- The average US data breach costs $9.44 million [1]
- 83% of data breaches occur in organizations that have had a breach before

Table Of Contents

Sources of Vulnerabilities

Code vulnerabilities come from the people who wrote that code

- Stopping active breaches requires removing vulnerable code
- Avoiding breaches altogether requires a different approach

Sources of Vulnerabilities

Best examples of each deficit using the numbers in original table [6].
I: Internal Factors, E: External Factors

No.	Internal Factor	Deficit
I1	Misconceptions	KD
I4	Misplaced Trust on Frameworks/APIs	KD
I6	Lack of Experience	KD
I9	Not handling cognitive load	AD
I11	Loss of Focus on Security	AD/ID
I12	Requires too much effort	ID
I15	Attitude of "Someone else's responsibility"	ID
I16	Attitude of "No one will notice/care"	ID

No.	External Factor	Deficit
E1	Inadequate information to be found	KD
E2	Lack of information sharing among teams	KD
E4	Poor division of labor	AD
E6	Limited resources	ID
E7	Lack of security culture	ID
E8	Lack of prioritization of security features	ID

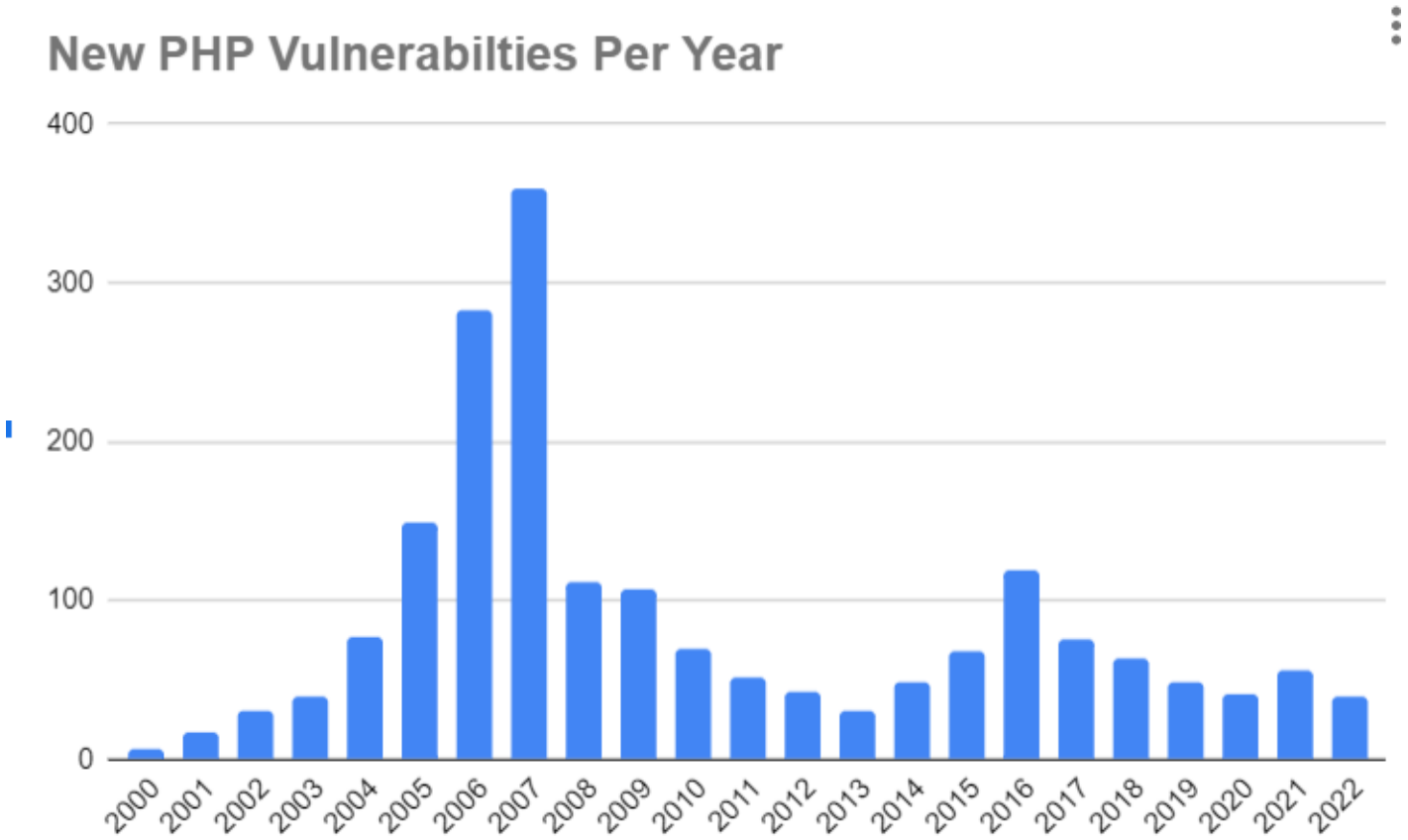
KD: Knowledge Deficit, AD: Attention Deficit, ID: Intention Deficit

Sources of Vulnerabilities

Knowledge Deficits

Sources of Vulnerabilities

Example of Knowledge Deficit



Sources of Vulnerabilities

More Examples of Knowledge Deficits

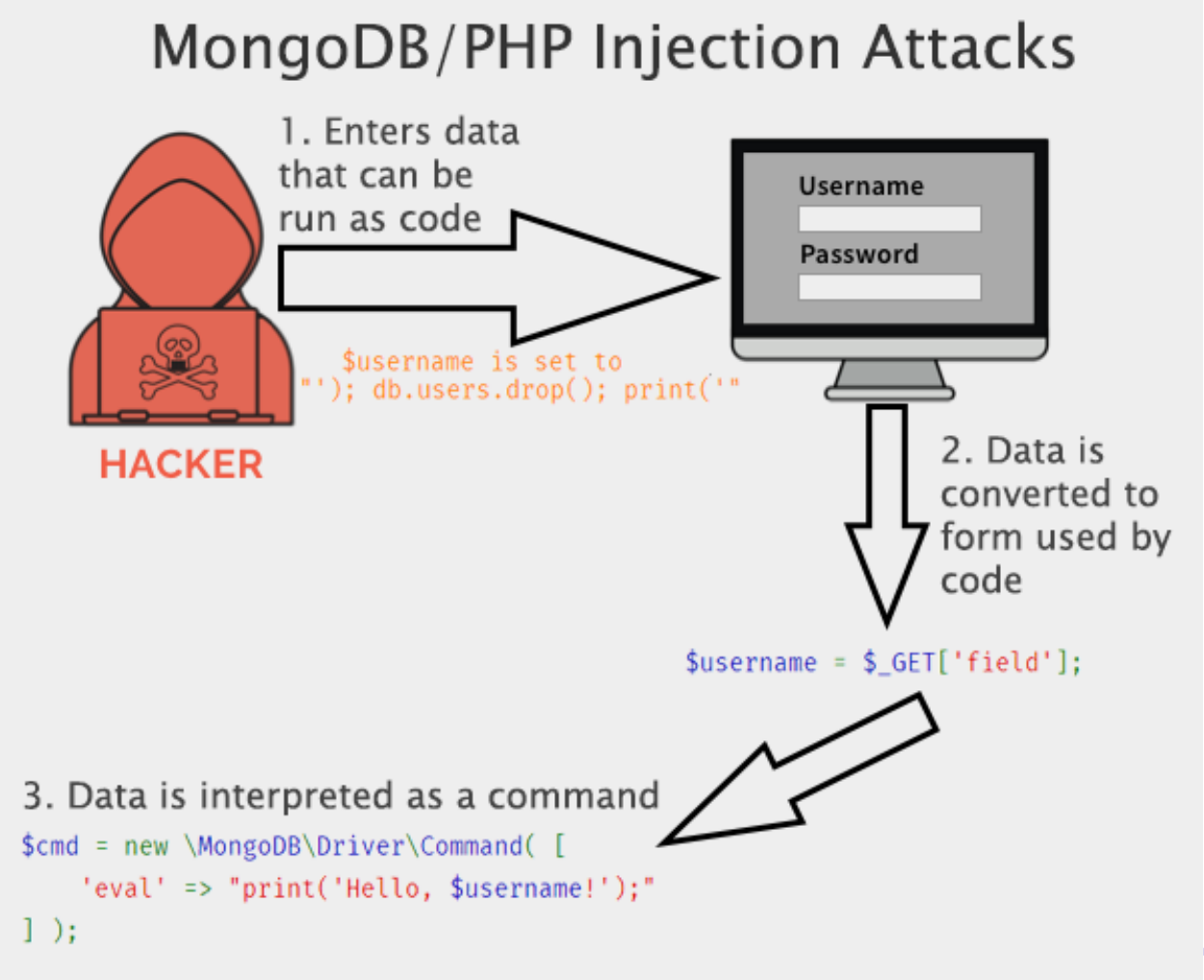
No.	Internal/External Factor
I1	Misconceptions
I2	Use of outdated information
I4	Misplaced Trust on Frameworks/APIs
I5	Lack of Domain Knowledge
I6	Lack of Experience
E1	Inadequate information to be found
E2	Lack of information sharing among teams

Sources of Vulnerabilities

Attention Deficits

Sources of Vulnerabilities

Example of Attention Deficit



Sources of Vulnerabilities

More Examples of Attention Deficits

I8	Not identifying security blind spots in tasks
I9	Not handling cognitive load
I10	Developer's Insecure Habits
E3	Task Complexity
E4	Poor division of labor
E6	Limited resources

Sources of Vulnerabilities

Intention Deficits

Sources of Vulnerabilities

Example of Intention Deficit

Most cars are not secure

"General interpretation today is that vehicles are vulnerable to many forms of failure if an attacker with malicious intent obtains access to susceptible vehicle components." [7]

Sources of Vulnerabilities

More Examples of Intention Deficits

I11	Loss of Focus on Security
I12	Requires too much effort
I13	Disregarding usefulness of secure practices
I14	Perceived lack of own security knowledge
I15	Attitude of "Someone else's responsibility"
I16	Attitude of "No one will notice/care"
E5	Absence of expectation of secure coding
E6	Limited resources
E7	Lack of security culture

Sources of Vulnerabilities

I: Internal Factors, E: External Factors

No.	Internal/External Factor	Deficit
I1	Misconceptions	KD
I4	Misplaced Trust on Frameworks/APIs	KD
I6	Lack of Experience	KD
I9	Not handling cognitive load	AD
I12	Requires too much effort	ID
I15	Attitude of "Someone else's responsibility"	ID
I16	Attitude of "No one will notice/care"	ID
E2	Lack of information sharing among teams	KD
E4	Poor division of labor	AD
E7	Lack of security culture	ID
E8	Lack of prioritization of security features	ID

KD: Knowledge Deficit, AD: Attention Deficit, ID: Intention Deficit

Table Of Contents

Security Interventions

Awareness Interventions

Security Interventions

Examples of Awareness Interventions

Forbes

AI

MORE Alarming Cybersecurity Stats For 2021 !

OWASP PROJECTS CHAPTERS EVENTS ABOUT Search OWASP.o

OWASP Top Ten

Main | Translation Efforts | Sponsors | Data 2020

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

Globally recognized by developers as the first step towards more secure coding.

Companies should adopt this document and start the process of ensuring that their web applications minimize these risks. Using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces more secure code.

Security Interventions

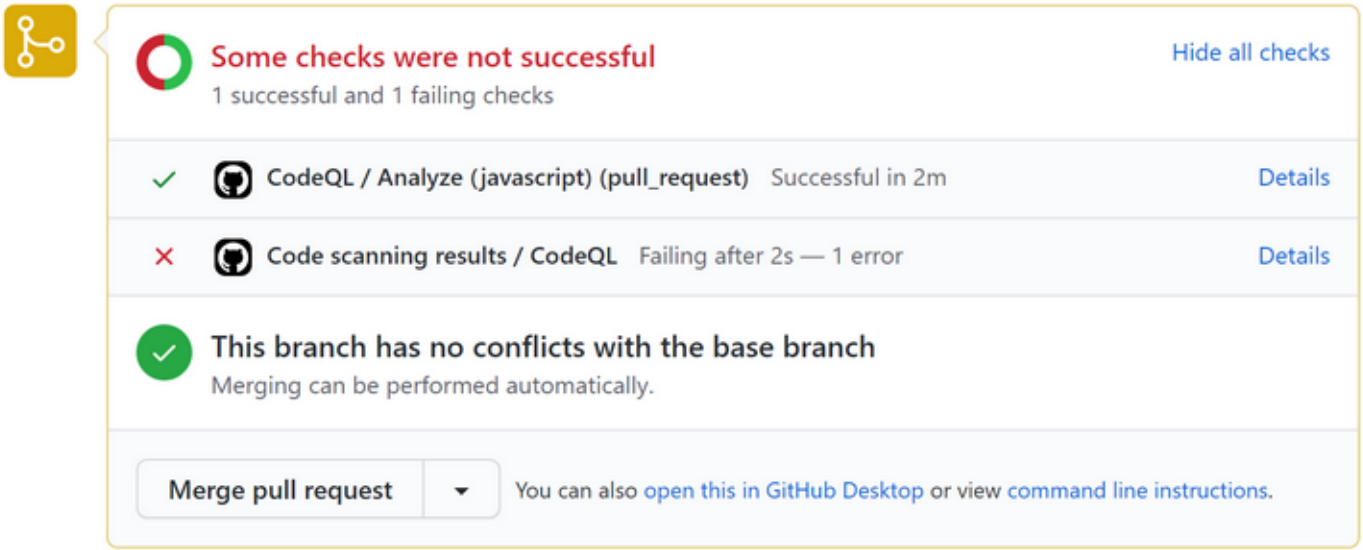
More Examples of Awareness Interventions

- Open Web Application Security Project
- Common Vulnerability and Exposures
- Info Pamphlets
- Vulnerability Databases
- Code Checklists
- Code Review

Automated Interventions

Security Interventions

Example of Automated Interventions



Security Interventions

Another Example of Automated Interventions

Security Interventions

More Examples of Automated Interventions

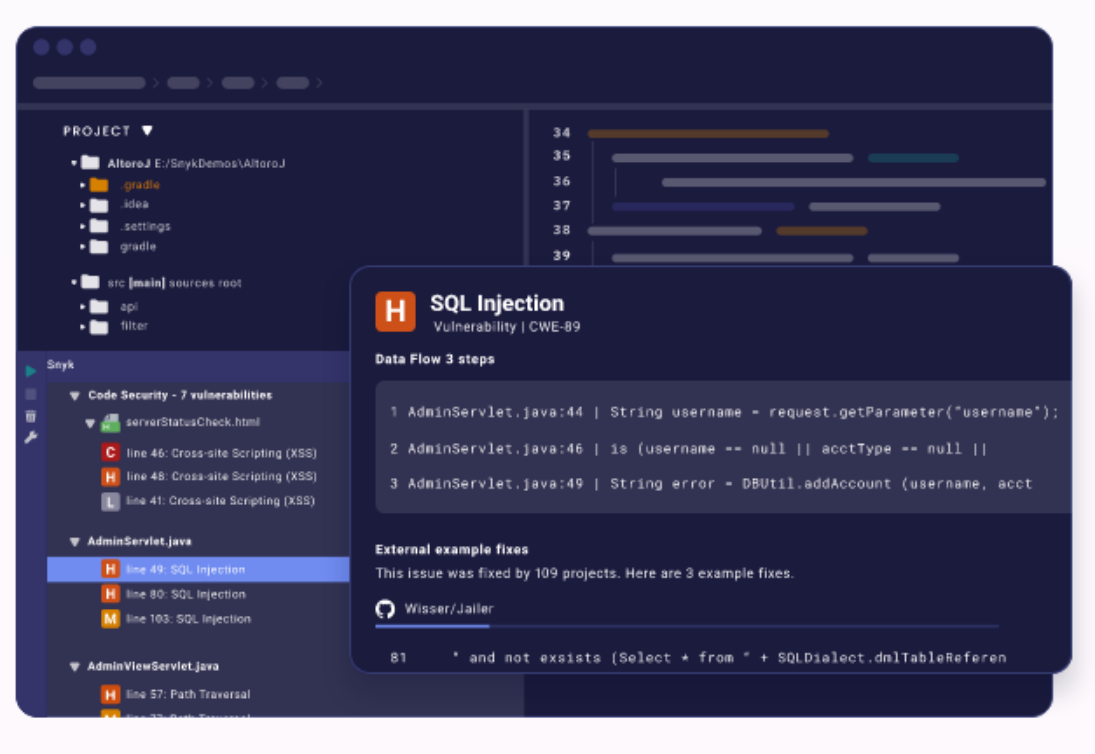
- Application Testing
- Vulnerability Prediction Tools
- Self-Written Tests

Interactive Interventions

Security Interventions

Example of Interactive Inervention

Snyk, So Now You Know



Security Interventions

More Examples of Interactive Interventions

- Snyk
- Fixdroid
- ASIDE
- PyCrypto API

Table Of Contents

Results

Comparing Security Interventions

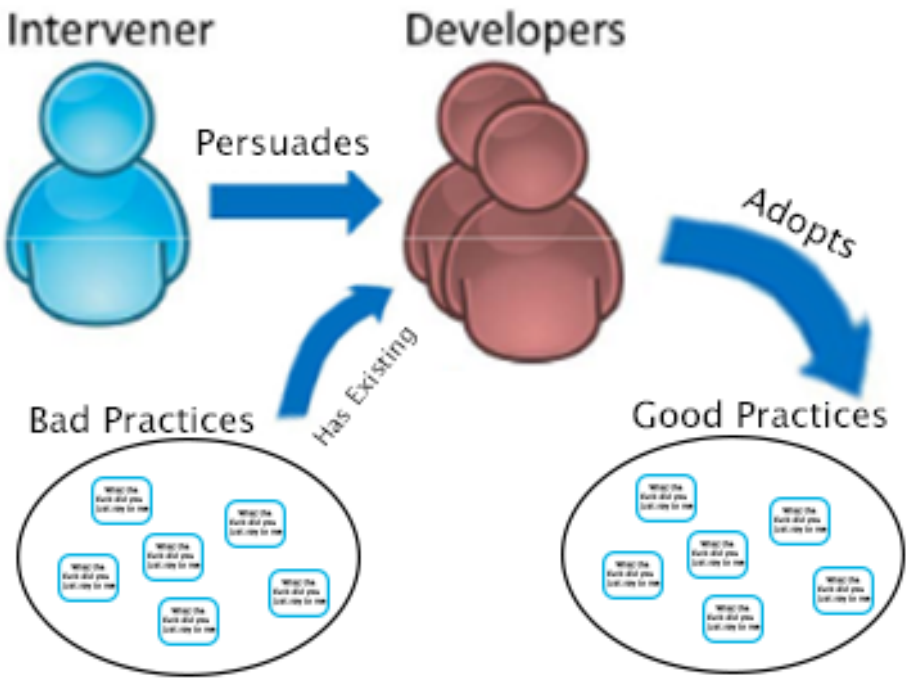


Figure: Weir, Becker, et al. found security interventions were most effective when centered around persuading the developer

Results

Comparing Security Interventions

Researchers Rauf, Petre, Tun, et al. qualitatively compared these interventions

	Awareness	Automated	Interactive
KD	✔	✔	✔
AD	×	✔	✔
ID	×	×	✔

KD: Knowledge Deficit, AD: Attention Deficit, ID: Intention Deficit

Results

Adopting Security Interventions

- Developers using Awareness Interventions produce better code [2]
- Automated Interventions catch potential breaches [6]

Results

Improving Security Interventions

- Do not assume your audience cares about security [5]
- Improve ease of access [4]
- Security is a cultural issue [6]

Questions

Bibliography I

[1] Cost of a data breach 2022.

[2] Y. Acar, M. Backes, S. Fahl, D. Kim, M. L. Mazurek, and C. Stransky.
You Get Where You're Looking for: The Impact of Information Sources on Code Security.
In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 289–305, May 2016.
ISSN: 2375-1207.

[3] C. Brooks.
MORE Alarming Cybersecurity Stats For 2021 !

Bibliography II

[4] Charles, C. Weir, I. Becker, J. Noble, L. Blair, M. A. Sasse, and A. Rashid.
Interventions for software security: creating a lightweight program of assurance techniques for developers.
In *Proceedings of the 41st International Conference on Software Engineering: Software Engineering in Practice*, ICSE-SEIP '19, pages 41–50, Montreal, Quebec, Canada, May 2019. IEEE Press.

Bibliography III

[5] T. B. Jordan, B. Johnson, J. Witschey, and E. Murphy-Hill.
Designing Interventions to Persuade Software Developers to Adopt Security Tools.
In *Proceedings of the 2014 ACM Workshop on Security Information Workers*, SIW '14, pages 35–38, New York, NY, USA, Nov. 2014. Association for Computing Machinery.

[6] I. Rauf, M. Petre, T. Tun, T. Lopez, P. Lunn, D. Van Der Linden, J. Towse, H. Sharp, M. Levine, A. Rashid, and B. Nuseibeh.
The Case for Adaptive Security Interventions.
ACM Transactions on Software Engineering and Methodology, 31(1):1–52, Jan. 2022.

Bibliography IV

[7] S. Stachowski, R. Bielawski, and A. Weimerskirch.
Cybersecurity Research Considerations for Heavy Vehicles.
Technical Report DOT HS 812 636, Dec. 2018.