Syzyfowe prace

wdrażanie OWASP Top 10 okiem web developera

Lena Sędkiewicz

O mnie

- Psycholog, terapeuta wyszkolony w nurcie TSR; WWO (https://www.icojarobietu.pl/)
- Pracowałam jako dziennikarka, copywriter, trener szermierki
- Napisałam 2 książki
- Od 2021 roku **Web Developer** sercem i ciałem
- Fanka F1 (Max!) i szydełkowania

https://www.linkedin.com/in/lena-sedkiewicz/

https://msedkiewicz.pl/

Web Developer

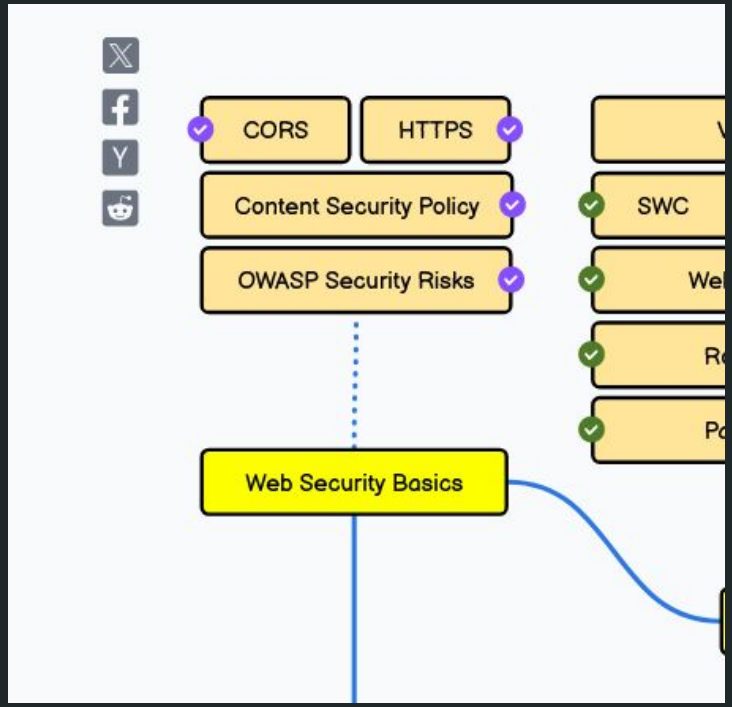
- Głównie frontend
- Trochę backend (WordPress)
- Na “froncie” - JS, React, Vue
- “Człowiek od stylowania” + pisanie kodu aplikacji
- Samouk + Bootcamp

Przyjrzyjmy się rozwojowi Frontendowca

Roadmapa dla Frontendowca

- Internet Basics > HTML > CSS > JS > Version Control System > Package Managers > Framework > More in depth CSS > Build Tools > Testing > Authentication Strategies > Web Security Basics

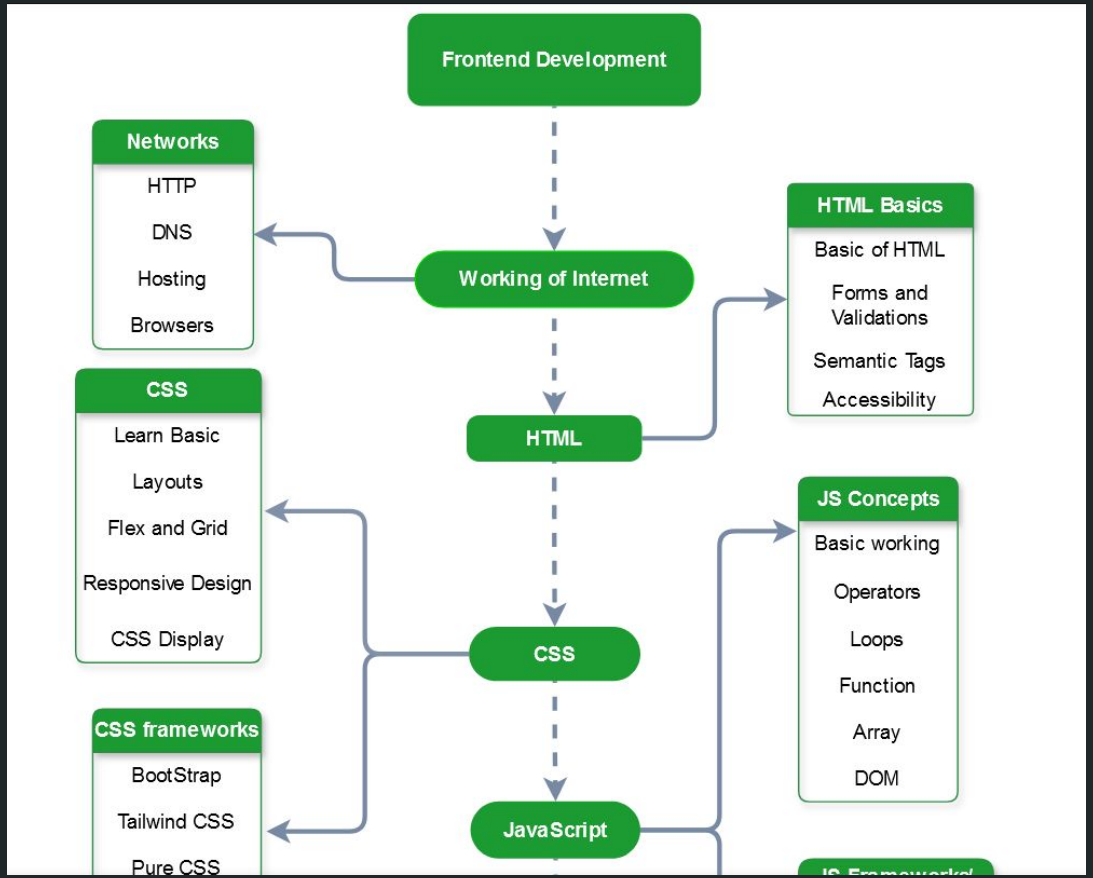
- https://roadmap.sh/frontend



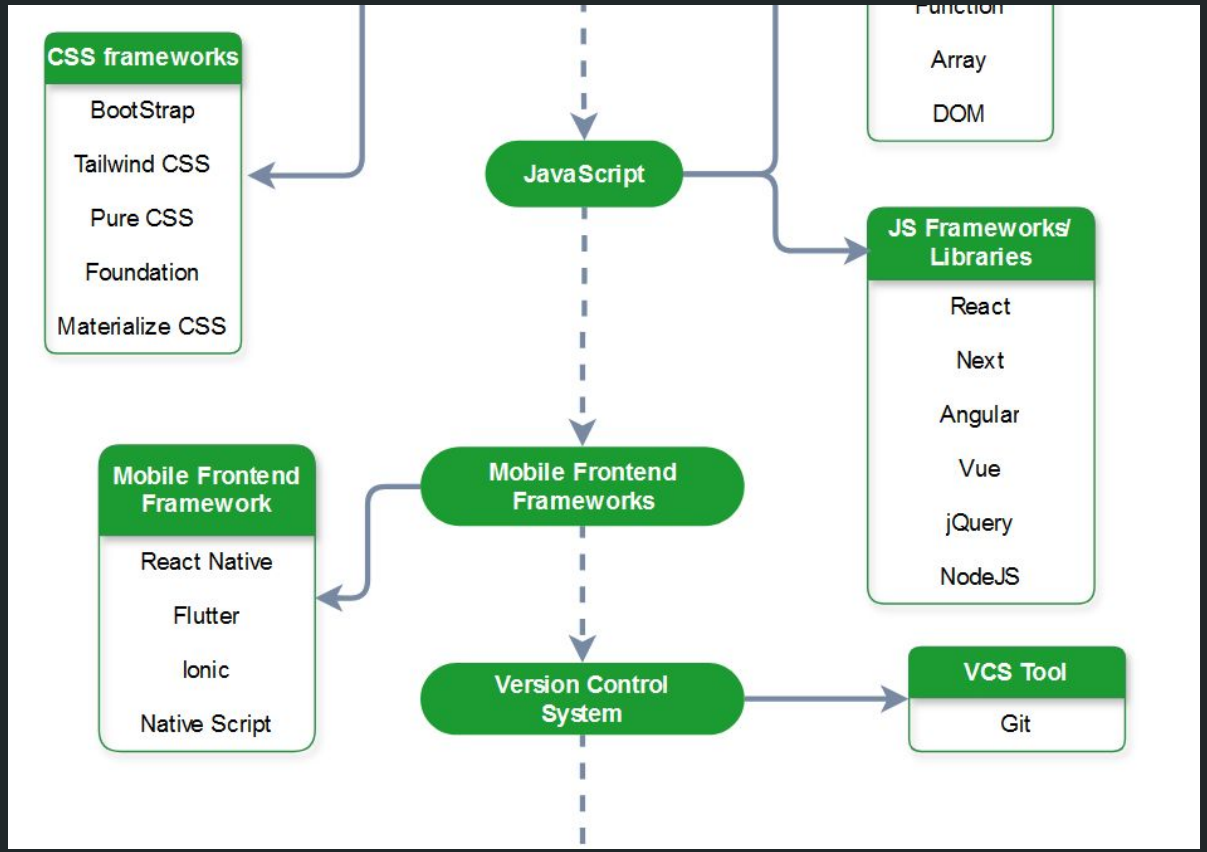
Roadmapa dla Frontendowca

- Internet Basics > HTML > Visual Studio Code > CSS > JS > Prompt Engineering > Version Control > Package Managers > Bootstrap 5 and SASS JavaScript Frameworks > Tailwind CSS > Build Tools > Testing > TypeScript > Web Security (OWASP)

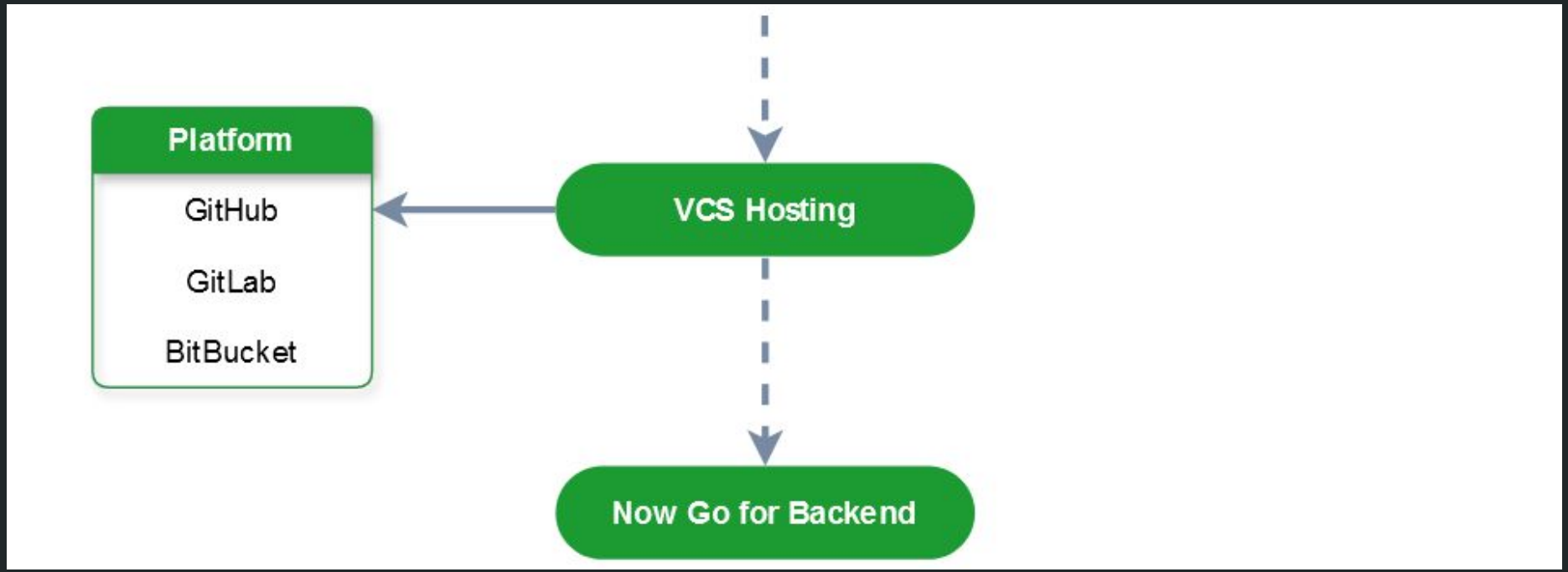
- https://www.freecodecamp.org/news/front-end-developer-roadmap/



https://www.geeksforgeeks.org/frontend-developer-roadmap/



https://www.geeksforgeeks.org/frontend-developer-roadmap/



https://www.geeksforgeeks.org/frontend-developer-roadmap/

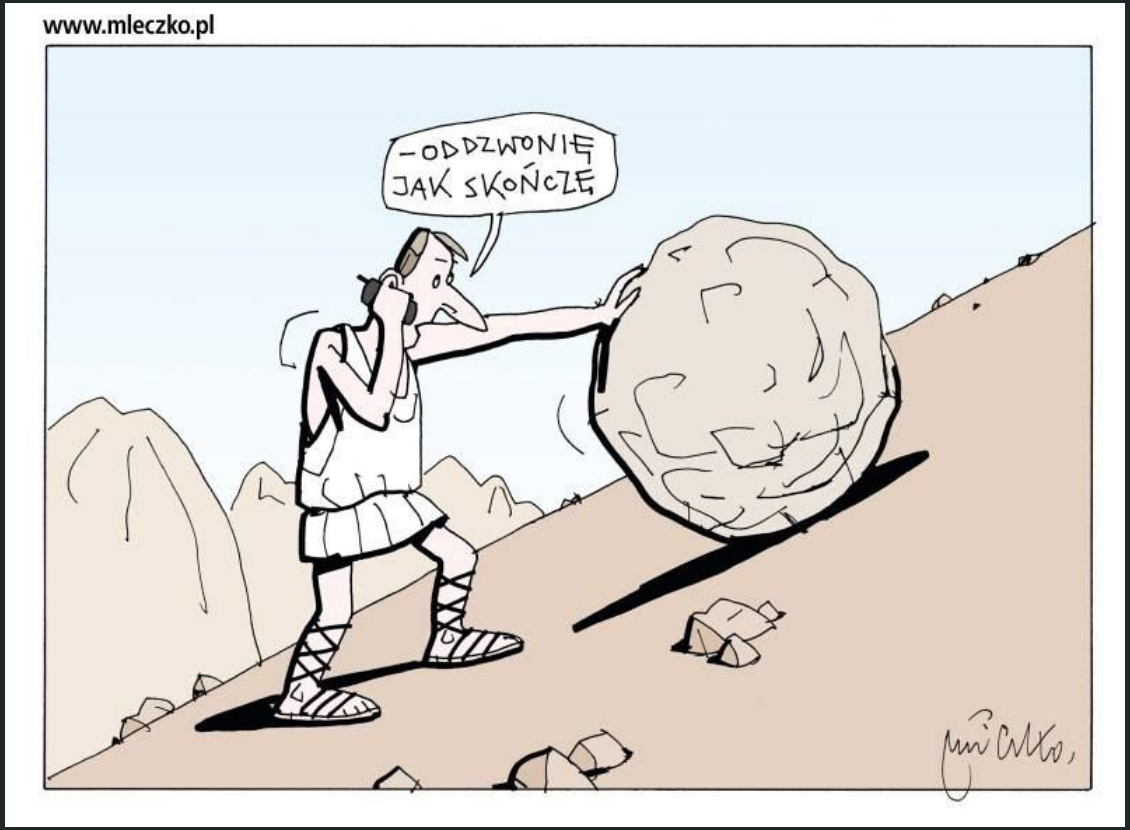
Sytuacja jest niewesoła...

Kontekst

- Problemy z powiązaniem przyczyn i skutków
  - Np. źle napisanego pod względem bezpieczeństwa kodu z incydentami
  - Np. braku edukacji w dziedzinie cyber u początkujących programistów z negatywnym postrzeganiem cyber na dalszej zawodowej drodze
- Konflikt “wojowników” i “kapłanów”
  - “Szybciej” vs. “bardziej przemyślanie”
- Nastawienie na szybki zysk / wynik / efekt
- Bezpieczeństwo kosztuje

Mindset

- Nastawienie na cel / wykorzystanie, niekoniecznie na lepszy kod
  - Choć jest przestrzeń do rozmów i zdobywania wiedzy
- Firmy szukają raczej “ukształtowanych” programistów
- Tempo zmian nie zawsze pozwala zgłębić temat security
- Przerzucanie się odpowiedzialnością (dev jest od pisania kodu...)
- Luki w edukacji (nie zawsze związane ze zmianą branży...)


www.mleczko.pl
-ODDZWONIĘ JAK SKOŃCZĘ

OWASP Top 10
w web developmencie

OWASP Top 10

- “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.”
- https://owasp.org/www-project-top-ten/

- Podnoszenie świadomości najbardziej krytycznych zagrożeń

OWASP Top 10 v. 2021

A01:2021
Broken Access Control

- Violation of the principle of least privilege or deny by default, where access should only be granted for particular capabilities, roles, or users, but is available to anyone.
- Bypassing access control checks by modifying the URL (parameter tampering or force browsing), internal application state, or the HTML page, or by using an attack tool modifying API requests.
- Permitting viewing or editing someone else's account, by providing its unique identifier (insecure direct object references)
- Accessing API with missing access controls for POST, PUT and DELETE.
- Elevation of privilege. Acting as a user without being logged in or acting as an admin when logged in as a user.
- Metadata manipulation, such as replaying or tampering with a JSON Web Token (JWT) access control token, or a cookie or hidden field manipulated to elevate privileges or abusing JWT invalidation.
- CORS misconfiguration allows API access from unauthorized/untrusted origins.
- Force browsing to authenticated pages as an unauthenticated user or to privileged pages as a standard user.

Konta użytkowników

- 2FA?
- Kolejne hasło do kolekcji?
- Brak edukacji (manager haseł)
- Customowo pisane rozwiązania vs. dostępne (np. w WordPress) - hardening?
- Wszyscy mają prawo mieć admina...
- Usuwanie starych kont?

- Ma być łatwo, miło i przyjemnie!

A02:2021
Cryptographic Failures

- Is any data transmitted in clear text? This concerns protocols such as HTTP, SMTP, FTP also using TLS upgrades like STARTTLS. External internet traffic is hazardous. Verify all internal traffic, e.g., between load balancers, web servers, or back-end systems.
- Are any old or weak cryptographic algorithms or protocols used either by default or in older code?
- Are default crypto keys in use, weak crypto keys generated or re-used, or is proper key management or rotation missing? Are crypto keys checked into source code repositories?
- Is encryption not enforced, e.g., are any HTTP headers (browser) security directives or headers missing?
- Is the received server certificate and the trust chain properly validated?
- Are initialization vectors ignored, reused, or not generated sufficiently secure for the cryptographic mode of operation? Is an insecure mode of operation such as ECB in use? Is encryption used when authenticated encryption is more appropriate?

- Are passwords being used as cryptographic keys in absence of a password base key derivation function?
- Is randomness used for cryptographic purposes that was not designed to meet cryptographic requirements? Even if the correct function is chosen, does it need to be seeded by the developer, and if not, has the developer over-written the strong seeding functionality built into it with a seed that lacks sufficient entropy/unpredictability?
- Are deprecated hash functions such as MD5 or SHA1 in use, or are non-cryptographic hash functions used when cryptographic hash functions are needed?
- Are deprecated cryptographic padding methods such as PKCS number 1 v1.5 in use?
- Are cryptographic error messages or side channel information exploitable, for example in the form of padding oracle attacks?

MD5...

1. Log into cPanel, launch phpMyAdmin and select your WordPress database from the list on the left.
2. Click on the `wp_users` table and find your user account in the list.
3. Click the **Edit** button for your user account. In the `user_pass` field, type your new password and choose MD5 from the function dropdown menu. Click **Go** to save the change.

https://10web.io/blog/how-to-change-wordpress-password/

HTTP

- Let’s Encrypt
- Dodanie reguł w .htaccess by wszystkie zasoby były serwowane po HTTPS
- Cloudflare i wymuszenie TLS 1.3
- Autoodnawianie certyfikatu (dobrze, by zespół wiedział...)
- SEOwcy lubią to (◠ ◡ ◠)

A03:2021
Injection

- User-supplied data is not validated, filtered, or sanitized by the application.
- Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter.
- Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records.
- Hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures.

Czas Twoim wrogiem...

- Pluginy, wtyczki, CMSy, frameworki, biblioteki...
- Korzystamy, bo “korzystają wszyscy”
- Doświadczenie pozwalające na dobrą sanityzację - CZAS!

- Junior napisze wszystko
- Współpraca Frontendowców i Backendowców

A04:2021
Insecure Design

Projektowanie systemu

- Brak współpracy
- Brak wiedzy o security
- Niechęć do implementacji security (“nas to nie dotyczy”)

Rozwijanie systemu

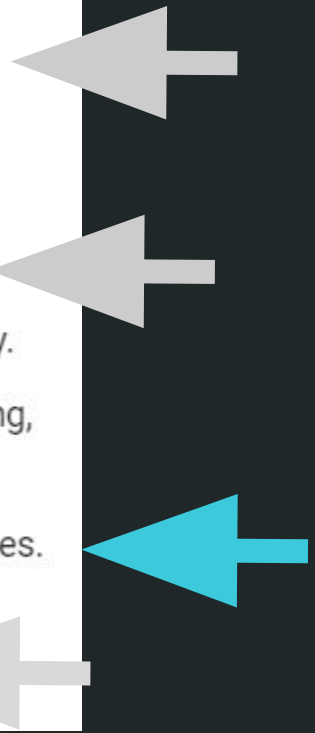
- Brak zmian w architekturze (jeśli są konieczne)
- “Łatanie” systemu “na ślinę”
- Zaciąganie długu technologicznego

Rekonesans / enumeracja

- Stack technologiczny
  - Trudności z ukryciem (sporo artefaktów)
  - Czas / budżet
  - Serwer też dużo zdradza...
- Współpraca Frontend Deva z Backend Devem?
- Znajomość logiki biznesowej jest ważna, ale...
- ... kto jest w stanie “z lotu ptaka” powiedzieć, co jest w aplikacji?
  - Bus factor => Zlepek factor
- Dokumentacja?
- Sekrety?

A05:2021
Security Misconfiguration

- Missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services.
- Unnecessary features are enabled or installed (e.g., unnecessary ports, services, pages, accounts, or privileges).
- Default accounts and their passwords are still enabled and unchanged.
- Error handling reveals stack traces or other overly informative error messages to users.
- For upgraded systems, the latest security features are disabled or not configured securely.
- The security settings in the application servers, application frameworks (e.g., Struts, Spring, ASP.NET), libraries, databases, etc., are not set to secure values.
- The server does not send security headers or directives, or they are not set to secure values.
- The software is out of date or vulnerable (see A06:2021-Vulnerable and Outdated Components).



Oczekiwania użytkownika vs. rzeczywistość

- Chcemy X ficzerów, ale skorzystamy z 10%
- Chcemy, by strona wyglądała ładnie, weźmiemy bibliotekę z której korzystamy w nikłym stopniu
- Dodamy kilka pluginów, nie zaszkodzi!

- Error handling? Nie ma czasu!

A06:2021
Vulnerable and Outdated Components

Oczekiwania użytkownika vs. rzeczywistość

- Aktualizacje?

- Brak czasu
- Brak wiedzy
- Niezrozumienie, jak szybko rozwija się technologa

https://www.wordfence.com/blog/,
https://solidwp.com/blog/category/wordpress-vulnerability-report/

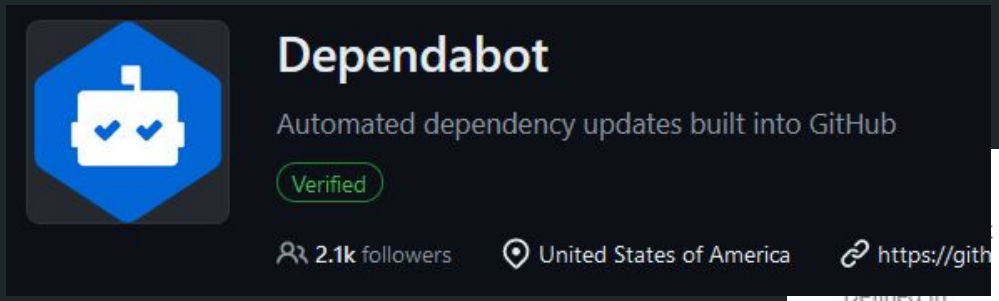
Zmiany w technologii

- WordPress - sam CMS, motywy, pluginy
- Porzucanie pewnych rozwiązań w CMS => zmiany w elementach zależnych (np. motywy)
- Zmiany w wersjach PHP
- Dynamicznie zmieniające się biblioteki i frameworki (np. React)

“Gotowe” rozwiązania

- Kto ma ocenić ich bezpieczeństwo?
- Kto ma powiedzieć - tu jest bezpieczniejsza biblioteka?
- A co jeśli ktoś “przechwyci” bibliotekę i doda złośliwą aktualizację?

- Jeśli dev nie śledzi, co się dzieje w cyber (bo np. ma i tak dużo pracy) => dowie się o ataku na łańcuch dostaw?



	Version	Upgrade to
	< 2.0.1	~> 2.0.1

package-lock.json

Vulnerabilities

CVE-2021-3803 High severity

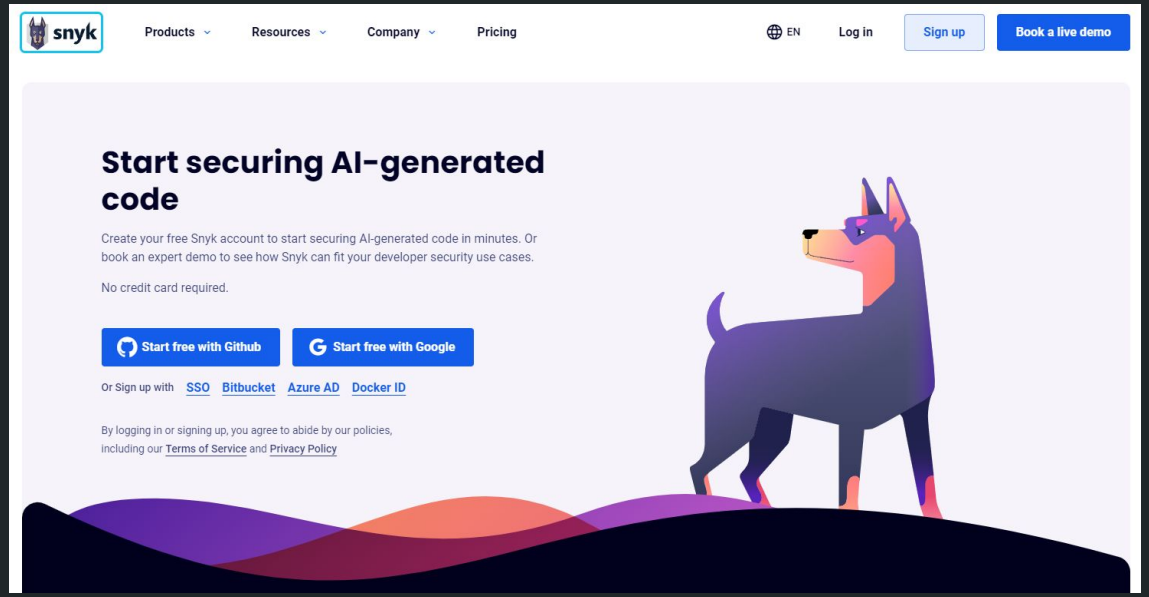
Dependency	Version	Upgrade to
webpack	>= 5.0.0 < 5.76.0	~> 5.76.0

Defined in

package-lock.json

Vulnerabilities

CVE-2023-28154 Critical severity



Project	Imported	Tested	Issues
package.json	Feb 28, 2023	5 hours ago	0 C 9 H 9 M 1 L
Code analysis	Feb 28, 2023	3 days ago	0 C 0 H 0 M 0 L

A07:2021 Identification and Authentication Failures

- Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords.
- Permits brute force or other automated attacks.
- Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin".
- Uses weak or ineffective credential recovery and forgot-password processes, such as "knowledge-based answers," which cannot be made safe.
- Uses plain text, encrypted, or weakly hashed passwords data stores (see A02:2021-Cryptographic Failures).
- Has missing or ineffective multi-factor authentication.
- Exposes session identifier in the URL.
- Reuse session identifier after successful login.
- Does not correctly invalidate Session IDs. User sessions or authentication tokens (mainly single sign-on (SSO) tokens) aren't properly invalidated during logout or a period of inactivity.

“Script Kiddies” w akcji

- Łatwo “wyłuskać” login
- Ograniczenie logowania z błędnym hasłem? Nic nie szkodzi, damy różne IP co 3 próby
- MD5?...
- Pluginy do podtrzymywania sesji dla WP...
- Pluginy do 2FA -> z dystansem
- Cloudflare? Niespecjalnie... (DDoS tak, ale Brute Force czy credential stuffing... hm)

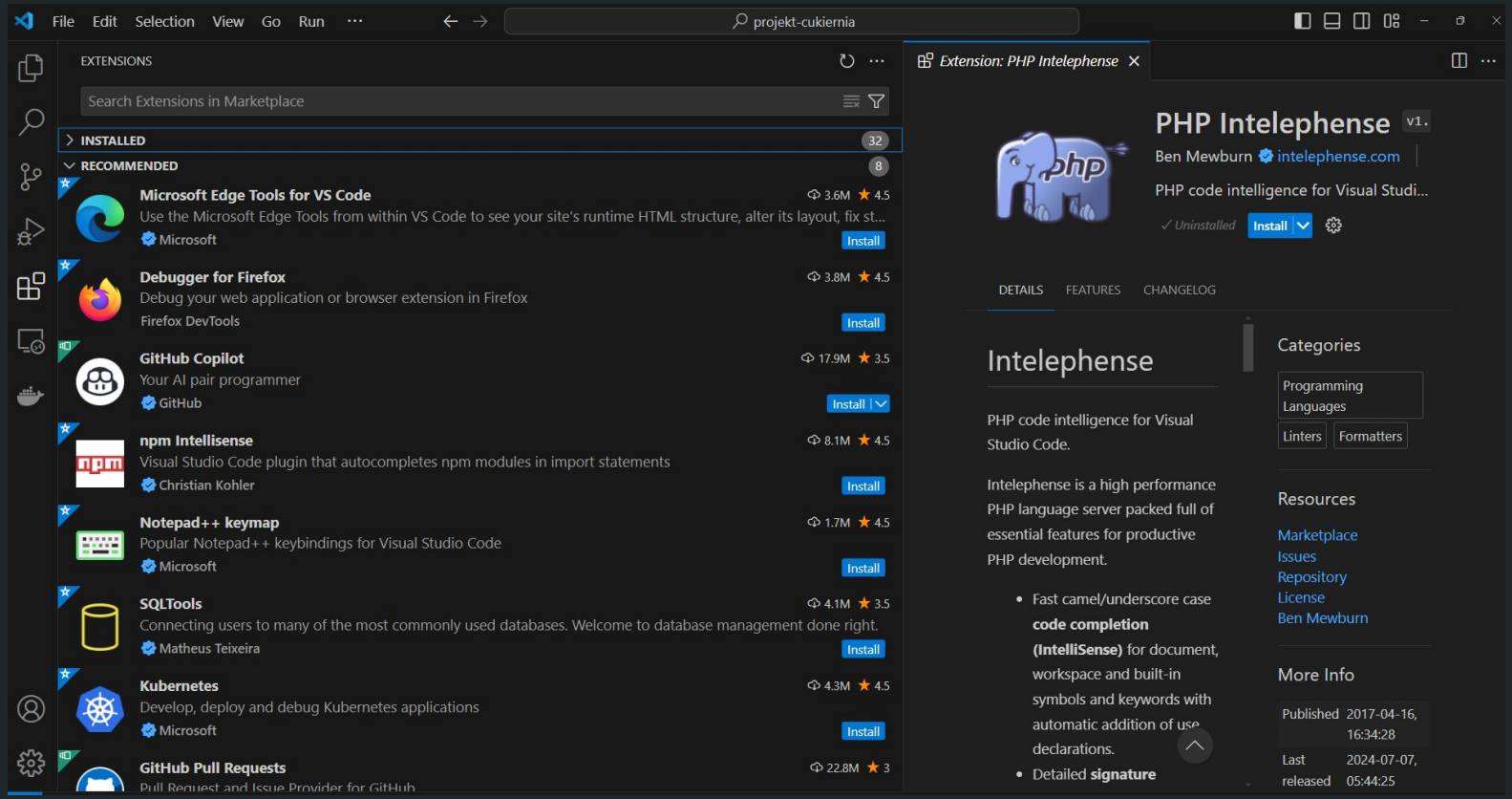

WordPress 2 Odebrane Failed login by IP 68.178.230.210 www.limitloginattempts.com -
WordPress 2 Odebrane Failed login by IP 51.145.159.13 www.limitloginattempts.com - Cz
WordPress Odebrane Failed login by IP 89.238.188.21 www.limitloginattempts.com - C
WordPress Odebrane Failed login by IP 8.217.191.150 www.limitloginattempts.com - Cz
WordPress Odebrane Failed login by IP 103.127.199.162 www.limitloginattempts.com -

A08:2021
Software and Data Integrity Failures

Potok CI / CD

- Zabezpieczenie własnego komputera
- Webpack
- Serwer
- Github
- Domena
- Dostęp do kont powiązanych z CI/CD
- CDN?...

PS: Czarna magia (⊗˜ o⊗˜) LUB brak dostępu


File Edit Selection View Go Run ···
projekt-cukiernia
EXTENSIONS
Search Extensions in Marketplace
INSTALLED 32
RECOMMENDED 8
Microsoft Edge Tools for VS Code
3.6M ★ 4.5
Use the Microsoft Edge Tools from within VS Code to see your site's runtime HTML structure, alter its layout, fix st...
Microsoft
Install
Debugger for Firefox
3.8M ★ 4.5
Debug your web application or browser extension in Firefox
Firefox DevTools
Install
GitHub Copilot
17.9M ★ 3.5
Your AI pair programmer
GitHub
Install
npm Intellisense
8.1M ★ 4.5
Visual Studio Code plugin that autocompletes npm modules in import statements
Christian Kohler
Install
Notepad++ keymap
1.7M ★ 4.5
Popular Notepad++ keybindings for Visual Studio Code
Microsoft
Install
SQLTools
4.1M ★ 3.5
Connecting users to many of the most commonly used databases. Welcome to database management done right.
Matheus Teixeira
Install
Kubernetes
4.3M ★ 4.5
Develop, deploy and debug Kubernetes applications
Microsoft
Install
GitHub Pull Requests
22.8M ★ 3
Pull Request and Issue Provider for GitHub
Extension: PHP Intelephense
PHP Intelephense
v1.
Ben Mewburn
intelephense.com
PHP code intelligence for Visual Studi...
Uninstalled
Install
DETAILS FEATURES CHANGELOG
Intelephense
PHP code intelligence for Visual Studio Code.
Intelephense is a high performance PHP language server packed full of essential features for productive PHP development.
Fast camel/underscore case code completion (IntelliSense) for document, workspace and built-in symbols and keywords with automatic addition of use declarations.
Detailed signature
Categories
Programming Languages
Linters
Formatters
Resources
Marketplace
Issues
Repository
License
Ben Mewburn
More Info
Published 2017-04-16, 16:34:28
Last released 2024-07-07, 05:44:25

A09:2021
Security Logging and Monitoring Failures

Returning to the OWASP Top 10 2021, this category is to help detect, escalate, and respond to active breaches. Without logging and monitoring, breaches cannot be detected. Insufficient logging, detection, monitoring, and active response occurs any time:

- Auditable events, such as logins, failed logins, and high-value transactions, are not logged.
- Warnings and errors generate no, inadequate, or unclear log messages.
- Logs of applications and APIs are not monitored for suspicious activity.
- Logs are only stored locally.
- Appropriate alerting thresholds and response escalation processes are not in place or effective.
- Penetration testing and scans by dynamic application security testing (DAST) tools (such as OWASP ZAP) do not trigger alerts.
- The application cannot detect, escalate, or alert for active attacks in real-time or near real-time.

Nowe skille dla programisty

- Sztuka czytania logów
- Narzędzia do czytania logów?
- Nadpisanie instalacji + brak logów

- ...a serwera to w ogóle proszę nie tykać!

Dostawca

A10:2021
Server-Side Request Forgery (SSRF)

SVG

- Niby dobry format....
- ...ale taki nie do końca.

Edukacja działu marketingu ¯_(ツ)_/¯

Jak żyć?

Życie web deva...

- Uczysz się tego, co Ci jest potrzebne na projekcie (i do zdobycia pracy)
- Zazwyczaj:
  - Technologia
  - SEO
  - (dostępność)
  - security

Punkt startowy

- Przestać przerzucać się odpowiedzialnością (Master of Obvious)
- Tworzenie przestrzeni spotkań
- Przesunięcie akcentu nauki cybersecurity wcześniej w rozwoju (przynajmniej podstaw teoretycznych)

Szukamy rozwiązań

- Edukacja własna
- Edukacja użyszkodników
- Edukacja biznesu
- Trochę mniejsze tempo pracy?

- Długa droga... do osobistej zmiany decydentów i programistów

Bezpiecznicy na meetupy!

Dla juniora (“spokojny” start)

- Kurs od Andrzeja Dyjaka (Ofensywne Testowanie Web Aplikacji)
- Kurs od Kacpra Szurka (Bezpieczny programista)
- Andrii Romasiun - WarsawJS 116 - Writing Secure JavaScript - https://www.hacksplaining.com/
- Język angielski...

Coś dla midów i seniorów (obowiązkowe)

- OWASP TOP 10
- OWASP Web Security Testing Guide (WSTG)
- OWASP Cheat Sheet Series (OCSS)
- OWASP Application Security Verification Standard (ASVS)

Dziękuję za uwagę!

https://www.linkedin.com/in/lena-sedkiewicz/

https://msedkiewicz.pl/