UTILIZAREA FRAMEWORKURILOR BACK-END ÎN SECURIZAREA APLICAȚIILOR WEB

Olivia DRUCEANU,
Facultatea de Matematică și Informatică

CZU: 004.056 *olivia.druceanu@gmail.com*

Odată cu dezvoltarea intensivă și progresivă a tehnologiilor, a afacerilor și a produselor, în paralel crește și numărul *aplicațiilor web*. Pentru a le crea în timp scurt, corect și pentru ca aplicațiile să fie cât mai securizate, sunt necesare instrumente mai performante, pentru a ușura lucrul dezvoltatorilor web.

Datele statistice arată că:

• 4 100 000 înregistrări de date au fost expuse la nivel global în prima jumătate a anului 2020, e-mailurile și parolele fiind primele pe listă [1, p. 3].

• Indicele de încălcare a securității datelor a arătat că frecvența medie a computerelor piratate este de 39 secunde sau de 2 244 de ori pe zi. Aceste dovezi cuantificabile au rezultat din experimentul în care securitatea slabă a fost configurată pe computere și toate atacurile au fost înregistrate [2].

• 46 000 de persoane au fost supuse atacului de tip „fishing", fiindu-le furate date personale. Se referă la moldovenii ce utilizau *facebook.com*, în primăvara anului 2019 [3].

Framework-urile backend, pe lingă rolul de creare a părții server a aplicațiilor web și de costruire a arhitecturii aplicației, și a bazei de date, asigură suplimentar securizarea acesteia.

Laravel rezpezintă un *framework MVC open source* ce poate fi utilizat pentru construirea, implementarea și rularea aplicațiilor *PHP*. El conține un manager de dependență dedicat și pachete modulare pentru a simplifica toate operațiunile. *Laravel* are capacitatea de a interacționa cu ușurință cu orice bază de date relațională și posedă instrumente de implementare a aplicațiilor. Din acest motiv se poate afirma că *Laravel* este un *framework PHP* utilizat foarte frecvent (Fig 1).

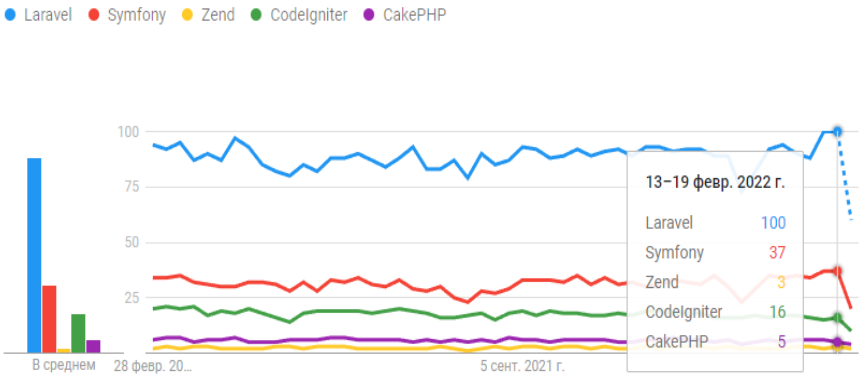

Fig. 1. Dinamica popularității framework-urilor backend bazate pe limbajul PHP [4].

Laravel oferă câteva mecanisme de securitate, pentru a permite dezvoltatorilor să reducă vulnerabilitățile din aplicațiile web:

- Este implementat sistemul de autentificare în *Laravel*;
- Sunt reduse vulnerabilitățile de tip *CSRF* (Cross Site Request Forgery);
- Există protecție împotriva atacurilor *XSS* (Cross Site Scripting);
- Este protecție împotriva injecțiilor SQL;
- Este îmbunătățită securitatea aplicațiilor în *Laravel*;
- Sunt implementate pachete de securitate *Laravel* [5];
- *Cookies* sunt securizate implicit – *Laravel* facilitează crearea, citirea și expirarea modulelor *cookie* cu clasa sa *Cookie*;
- Este utilizat *HTTPS* în procesul schimbului de date sensibile [6].

Poate fi menționat suplimentar, subsistemul robust de autentificare al utilizatorului din *Laravel*, cu codul standard asociat, disponibil în framework. *Laravel* folosește așa-numiții „furnizori” și „gardieni” pentru a facilita procesul de autentificare. Scopul „gardienilor” este autentificarea utilizatorilor pentru fiecare cerere pe care o fac, în timp ce „furnizorii” facilitează recuperarea datelor utilizatorilor din baza de date.

Dezvoltatorul, tot ce trebuie să facă, este configurarea bazei de date, a controlerelor și modelelor. În timpul procesului de dezvoltare, funcțiile de autentificare sunt încorporate în aplicație [5]

Concluzii. Odată cu creșterea numărului de utilizatori ai rețelei globale Internet și a volumului informației, este necesar de a crea sisteme calitative, ținând cont de experiențele avute de utilizatori.

Este important ca produsele web să fie construite cu respectarea standardelor de securitate.

Referințe:

1. Scurgerile de Informații, Raportul ENISA privind situația amenințărilor, Ianuarie 2019-aprilie 2020, Constatări, pag. 3*https://www.enisa.europa.eu/publications/report-files/ETL-translations/ro/etl2020-information-leakage-ebook-en-ro.pdf*
2. Statistici istorice privind încălcarea datelor [Citat: 05/03/2022]. Disponibil: https://www.varonis.com/blog/data-breach-statistics#:~:text=Over%20the%20past%2010%20years,months%20of%202019%20 (Forbes).
3. Moldoveni afectați de scurgeri de date personale din Facebook [Citat: 05/03/2022]. Disponibil: *https://www.mold-street.com/?go=news&n=11929*
4. Dinamica popularității framework-urilor backend bazate pe limbajul PHP [Citat: 05/03/2022]. Disponibil: *https://web.ceiti.md/lesson.php?id=17*
5. Caracteristici de securitate Laravel [Citat: 05/03/2022]. Disponibil: *https://www.cloudways.com/blog/laravel-security/?fbclid=IwAR1e2ogi_umwhz5GRE4lMjf6yQo5dpNYRpm25Kyejthvo07B-ZO51g5HVQc*
6. Caracteristici de securitate Laravel [Citat: 05/03/2022]. Disponibil:*https://www.tutorialspoint.com/laravel/laravel_security.htm*

Recomandat
Natalia PLEȘCA, conducător științific