УДК 004:38

**БЕЗПЕКА ВЕБ-ДОДАТКІВ. СУЧАСНИЙ СТАН. ЗАХИСТ ВІД ЗАГРОЗ.**

*Д.Ю. Лукашенко, студент,*

*А. І. Блозва, кандидат педагогічних наук, доцент*

В сучасну епоху Інтернету веб-програми стають все більш популярними та складними. Онлайн-сервіси забезпечують багато переваг. Малий бізнес, банки та великі промислові концерни залежать від веб-додатків. Поруч з цим залишаеється актуальним питання безпеки таких сервісів, оскільки зловмисники продовжують використовувати вразливості в додатках для доступу до конфіденційної інформації.

На сьогоднішній день визнаною світовою методологією оцінки вразливостей веб-додатків, що відображає сучасні тренди безпеки є OWASP «Топ-10» [1]. До цього топу відносяться наступні вразливості веб-додатків:



Рисунок 1 – Актуальний топ веб-вразливостей

Щорічно Acunetix аналізує дані, отримані від Acunetix Online, і складає звіт про тестування вразливостей. Цей звіт представляє стан безпеки веб-додатків. Звіт містить результати і аналіз вразливостей, виявлених за 12-місячний період з березня 2019 року по лютий 2020 року, на основі даних від 5000 цілей сканування.[2]



Рисунок 2 – Вразливості по рокам

Високий рівень вразливостей вказує на те, що зловмисник може повністю порушити конфіденційність, цілісність або доступність системи. 26 відсотків загроз високої серйозності - досить високий показник, але при цьому спостерігається зниження числа таких вразливостей з кожним роком. Типи вразливостей, що потрапляють в категорію висого ступеню небезпеки:



Рисунок 3 – Типи серйозних вразливостей

Брандмауер веб-додатків (Web Application Firewall) ModSecurity з встановленим основним набором правил OWASP (OWASP Core Rule set), які захищають від більшості мережевих атак (в тому числі, від OWASP Top Ten). При цьому Modsecurity встановлюється як додатковий модуль веб-серверу Apache, і може бути розгорнутий безпосередньо на сервері, який він захищає, або в режимі зворотнього проксі-серверу.

**Список використаних джерел:**

1. 10 Common Web Application Security Vulnerabilities and How to Prevent Them . [Електронний ресурс]. Режим достпупу: <https://relevant.software/blog/web-application-security-vulnerabilities/> (дата звернення 20.03.2021)

2. Acunetix Web Application Vulnerability Report 2020 [Електронний ресурс]. Режим доступу<https://www.acunetix.com/white-papers/acunetix-web-application-vulnerability-report-2020/> (дата звернення 05.04.2021).