МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет «Одеська юридична академія»

ЄВРОПЕЙСЬКІ ОРІЄНТИРИ РОЗВИТКУ УКРАЇНИ В УМОВАХ ВІЙНИ ТА ГЛОБАЛЬНИХ ВИКЛИКІВ XXI СТОЛІТТЯ: СИНЕРГІЯ НАУКОВИХ, ОСВІТНІХ ТА ТЕХНОЛОГІЧНИХ РІШЕНЬ

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

19 травня 2023 року

У двох томах

Том 1

Видавництво
«Юридика»
2023

УДК 005.332.2(4):316.42(477)"364""20"(062.552)
Є24

Рекомендовано до друку Вченою радою
Національного університету «Одеська юридична академія»
(протокол № 3 від 16.06.2023 р.)

За загальною редакцією **С. В. Ківалова.**

Відповідальний за випуск **М. Р. Аракелян.**
Матеріали видано в авторській редакції.

Є24 **Європейські** орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 19 травня 2023 р.) / за загальною редакцією С. В. Ківалова. – Одеса : Видавництво «Юридика», 2023. – Т. 1. – 790 с.

ISBN 978-617-8263-39-3

Матеріали Міжнародної науково-практичної конференції «Європейські орієнтири розвитку України в умовах війни та глобальних викликів XXI століття: синергія наукових, освітніх та технологічних рішень». У першому томі збірника містяться наукові напрацювання вчених, практиків, військовослужбовців у теоретичній та емпіричній площині в умовах повномасштабного військового вторгнення у сферах філософських основ, загальної теорії та історичних досліджень держави і права, актуальних проблем світових соціально-політичних процесів, соціології та психології. Висвітлено питання загроз національній безпеці в їхньому конституційному вимірі, у рамках міжнародного та європейського права, трудового права та права соціального забезпечення, земельного, аграрного та екологічного права, пов'язані з функціонуванням економіки та підприємництва в умовах європейського вибору України. Розглянуто проблеми інформатизації та цифровізації суспільства, захисту інформації та кібербезпеки в умовах військового вторгнення, питання методики викладання іноземних мов, теорії та практики перекладу, проблеми лінгвістики та журналістики.

Збірник розраховано на наукових та науково-педагогічних працівників, здобувачів вищої освіти, практичних працівників у сферах юридичної, економічної, соціологічної, політологічної, психологічної, філологічної наук, журналістики та кібербезпеки тощо.

УДК 005.332.2(4):316.42(477)"364""20"(062.552)

ISBN 978-617-8263-37-9 (у 2 т.)
ISBN 978-617-8263-39-3 (т. 1)

які невдовзі ми зможемо використовувати прямо на клієнтській стороні – у нашому браузері.

Список використаних джерел:

1. Burkhart N., Liao W., & Guzide O. (2020). An Overview of WebAssembly. *Proceedings of the West Virginia Academy of Science, 92(1)*. https://doi.org/10.55632/pwvas.v92i1.682
2. Ben L. Titzer. 2022. A fast in-place interpreter for WebAssembly. *Proc. ACM Program. Lang. 6, OOPSLA2*, Article 148 (October 2022), 27 pages. https://doi.org/10.1145/3563311
3. WebAssembly: як та чому. https://codeguida.com/post/1517
4. ASP.NET Core Blazor: https://learn.microsoft.com/uk-ua/aspnet/core/blazor/?WT.mc_id=dotnet-35129-website&view=aspnetcore-7.0
5. What is Pyodide? https://pyodide.org/en/stable/index.html

Ключові слова: веброзробка, вебпрограмування, веббраузер, JavaScript, WebAssembly.

Key words: web development, web programming, web browser, JavaScript, WebAssembly.

ТРОФИМЕНКО ОЛЕНА ГРИГОРІВНА

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент

МАНАКОВ СЕРГІЙ ЮРІЙОВИЧ

Національний університет «Одеська юридична академія»,
доцент кафедри інформаційних технологій, кандидат технічних наук

ПРОБЛЕМИ БЕЗПЕКИ ВЕБЗАСТОСУНКІВ

Нині за умов розповсюдження кіберзлочинів та проведення цілеспрямованих інформаційних війн вебресурси повсюдно піддаються атакам різного масштабу і складності з метою впливу на конфіденційність, цілісність і доступність даних інформаційних систем. Поширеність порушень безпеки сайтів та вебзастосунків, а також важливість їх запобігання зробило тестування безпеки невіддільною складовою життєвого циклу розробки відповідного програмного забезпечення (ПЗ), що має виявляти вразливості, пов'язані із забезпеченням цілісного підходу до захисту програми від хакерських атак, вірусів, несанкціонованого доступу до конфіденційних даних.

Тестування веббезпеки перевіряє бізнес-логіку, проблеми автентифікації та авторизації, кодування вхідних і вихідних даних, а також інші можливі ризики, щоб виявити уразливі місця в безпеці і переконатися, що всі функції вебзастосунків безпечні. Для тестування безпеки важливо враховувати різницю між ризиком та ефективністю

розроблених тестів безпеки щодо пом'якшення відповідного ризику безпеки для аналізу рентабельності інвестицій у безпеку [1]. Тестування безпеки вебпрограм допомагає імітувати та виявляти можливі уразливості та загрози, пов'язані з цією програмою. Воно перевіряє відповідність програми вимогам безпеки під час впливу будь-яких шкідливих вхідних даних.

Можливими проблемами, пов'язаними з аспектом вебтестування безпеки, є: зламані або ненадійні паролі, переповнення буфера, маніпулювання прихованими полями, ненадійне використання криптографії, перехоплення файлів cookie, неправильні конфігурації сервера, слабке керування сеансами, розкриття конфіденційних даних, маніпуляції з параметрами, соціальне хакерство, неадекватна перевірка введених даних тощо [1].

Проблеми, з якими стикається вебтестування безпеки, стосуються розробки автоматизованих інструментів для тестування веббезпеки, використання вебзастосунків RIA (Rich Internet Application), застосування незахищеного криптографічного сховища тощо [2]. Pentester має перевірити стійкість захисту ПЗ від різних невизначених атак, наприклад, від атак на відмову в обслуговуванні (DDoS attack), адже будь-яка уразливість може стати потенційно критичною загрозою для програми. Ризики безпеки вебзастосунку можуть бути пов'язані з фазою проєктування, фазою розробки, фазою розгортання, фазою технічного обслуговування. Саме тестування безпеки використовується для виявлення цих ризиків вебзастосунку, дослідження уразливостей і слабких місць вебпрограми. Наприклад, під час SQL-ін'єкції зловмисник може змінювати SQL-запити і в такий спосіб отримати неавторизований доступ до серверної частини. Ризик, пов'язаний із цією уразливістю, може полягати в тому, що зловмисник зможе отримати доступ до даних, на які він не авторизований.

Розробка автоматизованих інструментів завжди була проблемою тестування вебзастосунків на безпеку. Створити автоматизовані інструменти для тестування безпеки важче, ніж для тестування функціональності вебзастосунку [3]. Традиційні інструменти не встигають за темпами екосистеми програмного забезпечення. Проблеми, з якими стикаються автоматизовані інструменти для тестування веббезпеки, полягають у тому, що вони повинні йти в ногу з технологіями, що стрімко розвиваються та змінюються (наприклад, RIA), і належним чином інтегруватися в наявні робочі процеси розробки [4].

Зосередження на різних питаннях і проблемах, пов'язаних із тестуванням безпеки вебзастосунків, надає значні дивіденди у виявленні та усуненні різноманітних ризиків, уразливостей, атак, загроз, вірусів тощо. Крім того, корисно навчити тестувальника безпеки вміло моделювати тестову програму та розробляти відповідну стратегію тестування. Важливо розуміти і оцінювати рівень безпеки, який вимагатиме певний проєкт. Активи, які підлягають захисту, слід класифікувати і зазначенням їх рівня, наприклад: конфіденційно, секретно, цілком таємно. Також важливо переконатися, що усі законодавчі вимоги безпеки будуть дотримані у вебзастосунку та його оточенні, базуючись

на принципах конфіденційності, доступності та цілісності при зберіганні даних облікових записів, доступі і підключеннях користувачів. Управління ризиками безпеки й відповідність нормативним вимогам належать до політик і процесів, які організації мають забезпечити для дотримання законів, правил та нормативних актів.

Проведений аналіз проблем тестування вебзастосунків виявив наявність різних підходів для захисту програмних продуктів. Доволі не просто зорієнтуватися і зрозуміти, які саме методи використовувати або коли і в якій послідовності застосовувати ті чи інші засоби тестування. Доцільним є баланс у використанні декількох різних методів і підходів, які будуть доповнювати і посилювати один одного. Збалансований підхід до тестування безпеки залежить від багатьох чинників, у тому числі і зрілості процесу тестування та корпоративної культури, але важливо, щоб компанії приділяли увагу інтеграції тестування безпеки на якомога ранніх етапах життєвого циклу розробки ПЗ. Тестування безпеки має поєднувати різні ефективні техніки і методології для оцінки безпеки програми та її оточення.

Список використаних джерел:

1. Web Security Testing Guide. URL: https://owasp.org/www-project-web-security-testing-guide/stable/2-Introduction/
2. Keshav M. Automated VS Manual Security Testing – Which One to Choose? URL: https://www.getastra.com/blog/security-audit/manual-security-testing/
3. Трофименко О. Г., Пастернак Ю. Ю., Манаков С. Ю., Лобода Ю. Г. Автоматизація тестування вебсайтів електронної комерції. *Сучасна спеціальна техніка*. 2021. № 2(65). С. 46–59. DOI: 10.36486/mst2411–3816.2021.2(65).5
4. Trofymenko O. H., Dyka A. I. Problems of testing e-commerce websites. *International scientific conference «Information technologies and management in higher education and sciences»*: conference proceedings (November 28, 2022). Fergana, the Republic of Uzbekistan. Riga, Latvia: “Baltija Publishing”, 2022. Part 3. P. 195–199. DOI: 10.30525/978-9934-26-277-7-230

Ключові слова: тестування безпеки, вебзастосунок, безпека вебзастосунку, уразливості безпеки, засоби тестування.

Key words: security testing, web application, web application security, security vulnerabilities, testing tools.

ТОЛОКНОВ АНАТОЛІЙ АРНОЛЬДОВИЧ

Національний університет «Одеська юридична академія», асистент кафедри інформаційних технологій

ОГЛЯД МЕТОДІВ ЗАХИСТУ ВЕБФОРМ

Завдяки формам користувач «спілкується» з сайтом, вебсервісом: замовляє продукти, користується інтернет-банкінгом і просто автентифікується. Не треба говорити, що зберігання конфіденційної інформації, захист фінансової інформації – це одна з головних задач вебмайстра

СЕКЦІЯ 12
ІНФОРМАТИЗАЦІЯ ТА ЦИФРОВІЗАЦІЯ СУСПІЛЬСТВА В ЕПОХУ СТРІМКОГО РОЗВИТКУ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ