УДК 004.41:004.056

Коваленко О.В.
Центральноукраїнський національний технічний університет

ОЦІНКА ЕФЕКТИВНОСТІ ТЕХНОЛОГІЇ ТЕСТУВАННЯ БЕЗПЕКИ

У роботі проведені дослідження ефективності розробленої технології тестування безпеки додатків. Запропонована автором технологія тестування безпеки додатків включає в себе комплекс математичних моделей технології тестування Web-додатків. В основу математичного моделювання покладено підхід GERT-мережного синтезу. У результаті розроблено математичні моделі технології тестування DOM XSS уразливості і технології тестування уразливості до SQL ін'єкцій. Крім того, запропонована автором технологія тестування безпеки додатків включає в себе імітаційну модель технології тестування безпеки на основі положень теорії масштабування імітаційних моделей. Відмінною особливістю розробленої імітаційної моделі є адаптація вибору вхідних операторів управління і даних до підвищення вимог оперативності розробки та реалізації моделі, виражена в реалізації процедури взаємодії з реальним браузером із використанням засобів автоматизації браузера і формування даних для атаки на декількох діалектах. У даній роботі проведена оцінка достовірності отриманих результатів математичного моделювання.

Ключові слова: *тестування безпеки, масштабування імітаційних моделей, атаки на Web-додатки, GERT-мережі, технології тестування.*

Постановка проблеми. У роботах автора [1–12] розроблений комплекс математичних моделей технології тестування WEB-додатків. В основу математичного моделювання покладено підхід GERT-мережного синтезу. У результаті розроблено математичні моделі технології тестування DOM XSS уразливості і технології тестування уразливості до SQL ін'єкцій.

Математична модель технології тестування DOM XSS уразливості відрізняється від відомих, урахуванням виконання або аналізу DOM структури, що дає можливість провести аналітичну оцінку тимчасових витрат тестування зазначеної уразливості в умовах реалізації стратегії розробки безпечного програмного забезпечення. Математична модель технології тестування уразливості до SQL ін'єкцій відрізняється від відомих, вдосконаленим способом визначення відстані між результатами ін'єкції. Використання в запропонованому способі критерію Джаро-Вінклера, для порівняння результатів ін'єкції SQL коду і введення порогового значення дозволить підвищити точність результатів тестування безпеки програмного забезпечення.

У ході дослідження представлених моделей було визначено, що випадкова величина часу виконання розглянутих технологій тестування в цілому відповідає гамма-розподілу. Перевірка цієї гіпотези проведена за критерієм Пірсона.

У роботах автора [13; 14] отримала подальший розвиток імітаційна модель технології тестування безпеки на основі положень теорії масштабування імітаційних моделей. Відмінною особливістю розробленої імітаційної моделі є адаптація вибору вхідних операторів управління і даних до підвищення вимог оперативності розробки та реалізації моделі, виражена в реалізації процедури взаємодії з реальним браузером з використанням засобів автоматизації браузера і формуванні даних для атаки на декількох діалектах.

В основу запропонованого підходу алгоритмічного спрощення імітаційного моделювання покладені вдосконалені процедури оцінки транзитивної залежності з управління і даним. Визначено допустимість і доцільність використання оцінки транзитивної залежності, що знизить обчислювальну складність реалізованих алгоритмів у порівнянні з алгоритмами оцінки прямої залежності до 1,5 разів.

Метою роботи є оцінка ефективності розробленої технології в порівнянні з існуючими способами і технологіями, заснованими на відомому алгоритмі Пурдома, на основі проведеного імітаційного моделювання процесу тестування безпеки додатків [15, с. 256].

Практичний досвід тестування безпеки додатків показують, що визначення точних кількісних даних вразливостей додатків, як правило,

не представляється можливим з огляду на безліч невизначеностей вхідних даних. Тому широкого поширення набули наближені оцінки, засновані на обробці емпіричних даних, зібраних в процесі тестування безпеки.

У роботі в якості основи для оцінки ефективності розробленої технології тестування безпеки додатків використовуємо один із методів статистичного аналізу – зведення і групування статистичних даних, який отримав теоретичне обгрунтування в роботах [16, с. 217].

Під час проведення дослідження було взято 20 Web-додатків з різною кількістю (від 31 до 77) тестованих елементів.

У результаті експериментів отримані значень часу тестування безпеки додатків для способів, які використовують алгоритм Пурдома і розробленої технології тестування безпеки. Результати тестування представлені в табл. 1.

Побудуємо інтервальний ряд розподілу часу тестування безпеки, для чого виберемо оптимальний інтервал k і встановимо розмах інтервалу h. Оптимальне число груп виберемо так, щоб в достатній мірі відбилося різноманітність значень ознаки в сукупності і в той же час закономірність розподілу, його форма не змінювалась випадковими коливаннями частот, при цьому скористаємося формулою Стерждесса.

У нашому випадку оптимальний інтервал: $k = 1 + 3{,}322lg20 = 5{,}32$. Оскільки число груп не може бути дробовим, то округляємо $k = 5{,}32$ до найближчого цілого числа по правилам округлень – 5.

Знаючи число груп, розраховують довжину (розмах) інтервалу за формулою:

$$h = \frac{X_{\max} - X_{\min}}{k}.$$

Віходячи із даних, які визначені вище,

$$h1 = (52 – 11{,}1)/5 = 8{,}18$$
$$h2 = (48{,}7 – 11)/5 = 7{,}54.$$

Таким чином, інтервальний ряд розподілу часу тестувння безпеки розібємо на 5 груп з інтервалом по $8{,}18$ с. і $7{,}68$ с.

Представимо інтервальний ряд розподілення тестування безпеки додатків у вигляді табл. 2.

Як видно з наведеної таблиці, навіть настільки невелика вибірка тестованих додатків показала переваги розробленої технології тестування безпеки. Так, максимальне значення інтервального ряду менше під час використання розробки в 1,07 рази, зменшилася кількість влучень у максимальний часовий інтервал, а також сумарний час тестування менший в 1,05 рази.

Слід зауважити, що на практиці найчастіше не використовується теоретично обгрунтований алгоритм Пурдома. При цьому тестування безпеки проводиться виходячи з досвіду тестуваль-

Таблиця 1

Результати тестування безпеки Web-додатків

N	Час тестування (алг. Пурдома), с.	Час тестування (розроблена технологія тестування), с.	N	Час тестування (алг. Пурдома), с.	Час тестування (розроблена технологія тестування), с.
1	23	22,4	11	14,7	14,5
2	15,3	14,5	12	29,2	28,2
3	44	41,1	13	45,6	44,1
4	23,5	22,1	14	11,1	11
5	43,7	41,0	15	19,3	18,6
6	24,1	22,7	16	12,4	12
7	33	31,6	17	31,6	30,2
8	52	48,7	18	20,1	19.6
9	17,8	17,4	19	33,1	31,4
10	20,1	19,3	20	24	22,9

Таблиця 2

Інтервальний ряд розподілу тестування безпеки Web-додатків

Час (алг. Пурдома) (с.)	Число попадань в інтервал	Час (розроблена технологія тестування), с.	Число попадань в інтервал
11,1-19,28	5	11-18,54	5
19,28-27,46	7	18,54-26,08	7
27,46-35,64	4	26,08-33,62	4
35,64-43,82	1	33,62-41,16	2
43,82-52	3	41,16-48,7	2

ників. У цьому випадку розроблена технологія тестування має істотну перевагу (до 1,5 рази).

Для обґрунтування достовірності отриманих в роботах [1–14] результатів проведено ряд експериментів, відповідно до умов:

1) група тестувальників складається з 3 чол, з них два тестувальника безпеки і один Person Non [16, с. 152];

2) основна методологія управління розробкою є SCRUM;

3) число експериментів $N^* = 20$.

За результатами експерименту, отримана гістограма часу тестування безпеки додатків [17, с. 306] представлена на рис. 1.

Висунута гіпотеза про нормальний розподіл цієї випадкової величини була перевірена за критерієм узгодженості Пірсона [16, с. 98]

$$\chi^2 = N^* \sum_{i=1}^{k} (P_i^* - P_i)^2 / P_i,$$

де k – число розрядів (інтервалів) статистичного ряду;

P_i^* і P_i – «статистична» та теоретична ймовірності «попадання» заданого показника в i-й розряд.

Проведена перевірка довела правдоподібність гіпотези про те, що величина часу тестування безпеки додатків розподілена за нормальним законом.

Отримані оцінки $\hat{t}_{\text{тест}}^{(i)}$ математичного очікування та $\hat{D}_{t_{\text{тест}}^{(i)}}$ дисперсії ($\hat{\sigma}_{t_{\text{тест}}^{(i)}}$ середньоквадратичного відхилення) випадкової величини $t_{тест}^{(i)}$ часу тестування безпеки додатків [17, с. 298].

$$\hat{t}_{\text{тест}}^{(i)} = \frac{\sum_{i=1}^{k} \hat{t}_{\text{тест}}^{(i)}}{N^*}; \quad \hat{D}_{\hat{t}_{\text{тест}}^{(i)}} = \frac{\sum_{i=1}^{k} \left(\hat{t}_{\text{тест}}^{(i)} - t_{\text{тест}}^{(i)}\right)^2}{N^* - 1};$$

$$\hat{\sigma}_{\hat{t}_{\text{тест}}^{(i)}} = \sqrt{\hat{D}_{t_{\text{тест}}^{(i)}}}.$$

Скориставшись відомим виразом для розрахунку довірчої ймовірності відхилення відносної частоти від постійної ймовірності в незалежних дослідженнях [16, с. 312], визначимо довірчу ймовірність того, що отримане в результаті експерименту значення часу тестування безпеки додатків «не відхилена» від математичного очікування $\hat{t}_{\text{тест}}^{(i)}$ більш ніж на 1:

$$P\left(\left|\hat{t}_{\text{тест}}^{(i)} - t_{\text{тест}}^{(i)}\right| < 1\right) = 2\Phi\left(1 \Big/ \hat{t}_{\text{тест}}^{(i)}\right),$$

де Ф – функція Лапласа виду $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-t^2/2} dt$ [16, с. 316].

Результати перевірених експериментів показали, що для всіх досліджуваних видів даних довірча ймовірність того, що значення сатистичної величини $t_{тест}^{(i)}$ «не відхилиться» від математичного очікування $\hat{t}_{\text{тест}}^{(i)}$ більш ніж на 1 дорівнює: $P \approx 0{,}92$.

За даними, отриманим в роботах [13; 14], в умовах, зазначених вище, проведено порівняльне дослідження результатів математичного моделювання і експерименту. Результати порівняння представлені на рис. 2. у вигляді графіка щільності розподілу ймовірностей часу тестування безпеки додатків і відповідних їм кордонів довірчого інтервалу:

$$I_\beta = \left[\hat{\bar{J}} - \varepsilon_\beta, \hat{\bar{J}} + \varepsilon_\beta\right],$$

в якій істинне значення попадає з довірчою ймовірністю $\beta = 0{,}94$ і оцінок його матиматичного очікування.

З графіка видно, що в ключовій тестовій ситуації «розрахункова» крива (суцільна крива), отримана відповідно до розробленої в роботах [1–12] математичної моделі, в більшості практичних випадків потрапляють в «усереднений» довірчий інтервал (заштрихована область).

Це підтверджує достовірність розробленої в роботах [1–12] математичної моделі і отриманого в результаті математичного моделювання аналітичного виразу.

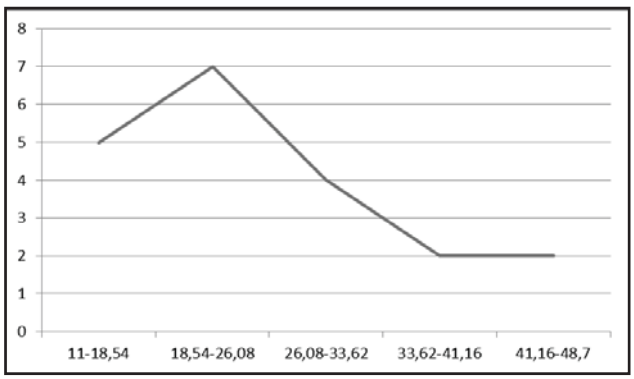

Рис. 1. Гіксограма часу тестування безпеки додатків

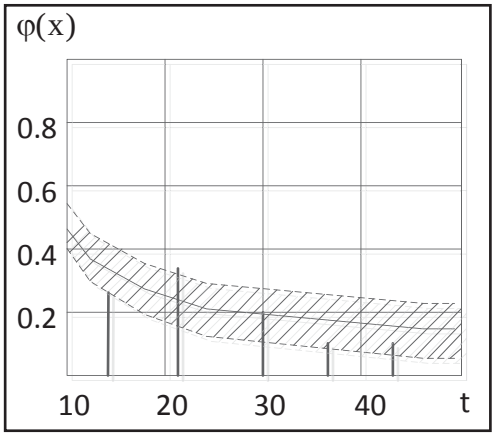

Рис. 2. Графік щільності розподілу ймовірностей часу $t_{тест}$ тестування системного ПЗ, відповідним їм межах довірчого інтервалу та оцінок його $\hat{t}_{\text{тест}}^{(i)}$ математичного очікування

Висновки. У роботі проведені дослідження ефективності розробленої технології тестування безпеки додатків і обґрунтування практичних рекомендацій щодо використання методів і засобів управління безпекою.

Визначено, що використання розробленої технології дозволить від 1,05 до 1,5 разів зменшити час тестування безпеки.

Під час оцінки достовірності отриманих у результаті математичного моделювання даних було проведено порівняння щільності розподілу ймовірностей часу тестування безпеки, відповідних їм кордонів довірчого інтервалу і оцінок його математичного очікування. Справжнє значення обраного показника потрапляє в довірчий інтервал із довірчою ймовірністю $\beta = 0{,}94$.

Список літератури:

1. Коваленко А.В. Технология тестирования DOM XSS уязвимости. Безпека інформації. 2017. № 2(23). С. 73.

2. Коваленко А.В. Технология тестирования уязвимости к SQL инъекциям. Системи управління, навігації та зв'язку. 2017. № 5(45). С. 66.

3. Коваленко А.В., Смирнов А.А. , Коваленко А.С., Смирнов С.А. Технология тестирования DOM XSS уязвимости. Научно-практический журнал кибербезопасности (SPCSJ). 2017. № 1. URL: http://journal.scsa.ge/ru/issues/2017/09/484.

4. Коваленко А.В., Смирнов А.А., Коваленко А.С. Алгоритм анализа DOM XSS уязвимости при управлении рисками разработки программного обеспечения. Комбінаторні конфігурації та їх застосування: праці міжнар. наук.-техн. семінару. (Кропивницький, 7-8 квітня 2017 р.). Кропивницький, 2017. С. 125.

5. Коваленко А.В., Смирнов А.А., Коваленко А.С. Алгоритм анализа уязвимости SQL Injection для управления рисками разработки программного обеспечения. Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі: праці міжнар. наук.-техн. конф. (ПНПЗК-2017) (Харків, 10-12 квітня 2017 р.). Харків, 2017. С. 27.

6. Коваленко А.В., Смирнов А.А., Коваленко А.С. Алгоритмы анализа DOM XSS уязвимости и уязвимости SQL Injection при управлении рисками разработки программного обеспечения. Проблеми і перспективи розвитку ІТ-індустрії: праці IX міжнар. наук.-практ. конф. (Харків, 20-21 квітня 2017 р.). Харків, 2017. С. 61.

7. Kovalenko O.V., Smirnov O.A., Kovalenko A.S., Smirnov S.A. Method of testing the dom XSS vulnerability. Information technologies, systems and networks ITSN-2017: International Conference (Chisinau, Republic of Moldova. 17 – 18 October 2017). Chisinau, 2017. P. 7.

8. Коваленко О.В., Смірнов О.А., Коваленко А.С. , Смірнов С.А. . Метод тестування DOM XSS уразливості. Автоматика та комп'ютерно-інтегровані технології у промисловості, телекомунікаціях, енергетиці та транспорті: праці всеукр. наук.-практ. інтернет-конференції (Кропивницький, 16-17 листопада 2017 р.). Кропивницький, 2017. С. 198.

9. Коваленко О.В., Смірнов О.А., Коваленко А.С., Смірнов С.А.. GERT-модель технології тестування DOM XSS уразливості. Актуальні питання забезпечення кібернетичної безпеки та захисту інформації: праці IV міжнар. наук.-практ. конф. (Київ. 21-24 лютого 2018 р.). Київ, 2018. С. 65.

10. Коваленко О.В., Смірнов О.А., Коваленко А.С., Смірнов С.А. Технології тестування уразливостей Web-застосунків з використанням GERT-моделі. Комп'ютерні інтелектуальні системи та мережі (KICM-2018): праці всеукр. наук.-практ. конф. (Кривий Ріг, 21-23 березня 2018р.), Кривий Ріг, 2018. С. 5.

11. Коваленко А.В., Смирнов А.А. , Коваленко А.С. , Смирнов С.А. Тестирование уязвимости Web-приложений к атаке вида межсайтовый скриптинг. Securitea informationala 2018: Conferenta internationala (editia a XIV-a). (Chisinau, Moldova, 20-21 martie 2018). Chisinau, 2018. P. 54.

12. Коваленко А.В., Смирнов А.А. , Коваленко А.С., Смирнов С.А. Комплекс математических моделей технологии тестирования WEB-приложений. Проблеми і перспективи розвитку ІТ-індустрії: праці X міжнар. наук.-практ. конф. (Харків, 19-20 квітня 2018 р.). Харків, 2018. С. 16

13. Коваленко А.В. Масштабирование имитационной модели технологии тестирования безопасности. Системи управління, навігації та зв'язку. 2017. № 6(46). С. 181.

14. Коваленко А.В. Имитационная модель технологии тестирования безопасности Web-приложений. Системи управління, навігації та зв'язку. 2018., № 1(47). С. 114–123.

15. Томас Х. Кормен, Чарльз И. Лейзерсон, Рональд Л. Ривест, Клиффорд Ш. Алгоритмы. Построение и анализ. Вильямс, 2016. 1328 с.

16. Гмурман В.Е. Теория вероятностей и математическая статистика. Москва, 2003. 479 с.

17. Канер С. Тестирование программного обеспечения. Фундаментальные концепции менеджмента бизнес-приложений. Киев, 2001. 544 с.

ОЦЕНКА ЭФФЕКТИВНОСТИ ТЕХНОЛОГИИ ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ

В работе проведены исследования эффективности разработанной технологии тестирования безопасности приложений. Предложенная автором технология тестирования безопасности приложений включает в себя комплекс математических моделей технологии тестирования WEB-приложений. В основу математического моделирования положен подход GERT-сетевого синтеза. В результате разработаны математические модели технологии тестирования DOM XSS уязвимости и технологии тестирования уязвимости к SQL инъекциям. Кроме того, предложенная автором технология тестирования безопасности приложений включает в себя имитационную модель технологии тестирования безопасности на основе положений теории масштабирования имитационных моделей. Отличительной особенностью разработанной имитационной модели является адаптация выбора входных операторов управления и данных к повышению требований оперативности разработки и реализации модели, выраженная в реализации процедуры взаимодействия с реальным браузером с использованием средств автоматизации браузера и формирования данных для атаки на нескольких диалектах. В данной работе проведена оценка достоверности полученных результатов математического моделирования.

Ключевые слова: *тестирование безопасности, масштабирование имитационных моделей, атаки на Web-приложения, GERT-сети, технологии тестирования.*

EVALUATION OF THE EFFECTIVENESS OF SECURITY TESTING TECHNOLOGY

In this work, the studies were conducted on the effectiveness of the developed technology of application security testing. The technology offered by the author for application security testing includes a set of mathematical models of testing technology for WEB applications. The basis of mathematical modeling is the approach of GERT-network synthesis. As a result, mathematical models of testing technology for DOM XSS vulnerability and SQL injections have been developed. In addition, the application security testing technology proposed by the author includes a simulation model of security testing technology based on the theory of scaling of simulation models. A distinctive feature of the developed simulation model is the adaptation of the choice of input control operators and data to an increase in the requirements for the rapid development and implementation of the model, expressed in the implementation of the procedure for interacting with a real browser using browser automation tools and generating attack data in several dialects. In this work, the reliability of the results of mathematical modeling is estimated.

Key words: *security testing, scaling of simulation models, attacks on Web-applications, GERT-networks, technology testing.*