УДК 004.41:004.056 DOI: https://doi.org/10.32515/2664-262X.2019.2(33).173-180

О.В. Коваленко, доц., канд. техн. наук
Центральноукраїнський національний технічний університет, м. Кропивницький, Україна
e-mail: clashav@gmail.com

Математична модель технології тестування комплексу DOM XSS вразливостей для аналітичної оцінки часових витрат

В роботі представлені результати дослідження та алгоритми тестування на вразливість до одних з найбільш поширених видів атак на Web-застосунки – DOM XSS для аналітичної оцінки тимчасових витрат. В цілому, проведені дослідження показали, що GERT-моделювання є ефективним способом визначення заздалегідь невідомих законів і функцій розподілу випадкових величин при відомому алгоритмі функціонування (процесу). Головною метою GERT є оцінка логіки мережі і тривалість активності і отримання висновку про необхідність виконання деяких активностей. В результаті розроблено математичну модель технології тестування комплексу DOM XSS вразливостей яка відрізняється від відомих, урахуванням специфіки комплексного аналізу різних типів XSS вразливості («stored XSS», «reflected XSS» і DOM Based XSS), а також включенням в алгоритм процедур автоматичного аудиту DOM Based XSS окремо. Це дає можливість провести аналітичну оцінку тимчасових витрат тестування зазначених вразливостей в умовах реалізації стратегії розробки безпечного програмного забезпечення.

технології тестування, DOM XSS вразливості, GERT-моделювання, вразливості безпеки

А. В. Коваленко, доц., канд. техн. наук
Центральноукраинский национальный технический университет, г. Кропивницкий, Украина

Математическая модель технологии тестирования комплекса DOM XSS уязвимостей для аналитической оценки временных затрат

В работе представлены результаты исследования и алгоритмы тестирования на уязвимость к одним из наиболее распространенных видов атак на Web-приложения – DOM XSS для аналитической оценки временных затрат. В целом, проведенные исследования показали, что GERT-моделирование является эффективным способом определения заранее неизвестных законов и функций распределения случайных величин при известном алгоритме функционирования (процесса).Главной целью GERT является оценка логики сети и продолжительность активности и получения заключения о необходимости выполнения некоторых активностей.В итоге разработана математическая модель технологии тестирования комплекса DOM XSS уязвимостей которая отличается от известных, учетом специфики комплексного анализа различных типов XSS уязвимости («stored XSS», «reflected XSS» и DOM Based XSS), а также включением в алгоритм процедур автоматического аудита DOM Based XSS отдельно. Это дает возможность провести аналитическую оценку временных затрат тестирования указанных уязвимостей в условиях реализации стратегии разработки безопасного программного обеспечения.

технологии тестирования, DOM XSS уязвимости, GERT-моделирование, уязвимости безопасности

Постановка проблеми. Збільшення числа користувачів всесвітньої мережі Інтернет, постійне зростання інформаційного, фінансового і ділового контенту в кіберпросторі обумовлює підвищення попиту на Web-застосунки. У той же час цей процес викликає зворотню негативну реакцію з боку зловмисників, що мають постійну можливість аналізу об'єктивно існуючих вразливостей інтернет-застосунків.

Аналіз різного роду статистичних матеріалів відомих організацій (наприклад, Open Web Application Security Project) [1] показав, що одним з найбільш небезпечних видів атак (вразливостей) є міжсайтовий скриптинг – XSS (Cross Site Scripting).

Аналіз останніх досліджень і публікацій. З робіт [2, 3, 4, 5] відомо, що під XSS зазвичай мається на увазі моментальний і відкладений міжсайтовий скриптинг. При моментальному XSS зі шкідливим кодом (Javascript) повертається атакується сервером негайно як відповідь на HTTP запит. Відкладений XSS означає, що це шкідлива програма зберігається на системі, що атакується і пізніше може бути впроваджений в HTML сторінку вразливої системи. Така класифікація передбачає, що фундаментальна властивість XSS полягає в тому, що це шкідлива програма відправляється з браузера на сервер і повертається в цей же браузер (моментальний XSS) або будь-який інший браузер (відкладений XSS).

У ряді інтернет-статей [6, 7] детально описані основні механізми виникнення подібного роду погроз, а також шляхи можливого блокування. Однак, щоб ідентифікувати ці загрози і можливі наслідки їх поширення в процесі безпечного управління IT-проектами, а також запропонувати оптимальні шляхи вирішення цієї проблеми, існує необхідність математичної формалізації процесу їх ініціалізації і поширення.

У ряді робіт реалізовані спроби математичної формалізації процесу пошуку і усунення вразливостей подібного роду. Так в роботах [7] представлені узагальнені матеріали механізмів і процедур безпечного програмування, які переслідують цілі зниження ризиків вразливості. У роботах [8] представлені математичні моделі, які описують алгоритми аналізу Web-застосунків (в тому числі і алгоритм однією з найбільш поширених вразливостей – DOM (Document Object Model) XSS вразливості). Однак представлені моделі не враховують останні тенденції XSS вразливості, а саме відмінність їх типів («stored XSS», «reflected XSS» і DOM Based XSS) і необхідність їх виявлення.

Постановка завдання. Саме тому особливо актуальним завданням в цьому напрямку є моделювання алгоритму виявлення DOM (Document Object Model) XSS вразливості з урахуванням комплексу трьох їх можливих типів.

Проведені дослідження показали, що уразливість DOM XSS є підвид XSS, в разі якої результат атаки знаходиться не у відповіді сервера і, відповідно, не в HTML коді, а в DOM структурі HTML сторінки. При цьому в режимі «stored XSS» здійснюється передача і зберігання XSS на сервері. Надалі ми на цю сторінку перенаправляються користувачі. У режимі «reflected» XSS повертається в тілі відповіді від сервера на конкретний запит з самої XSS. Результати атак за допомогою таких вразливостей можна виявити тільки в процесі виконання або аналізі DOM структури. Сам механізм атаки, а саме ін'єкція Javascript коду в вразливий сегмент, залишається незмінним.

Одним з найменш математично формалізованих і досліджуваних типів XSS є DOM Based XSS. Можливо, це пов'язано з тим, що навіть сучасними сканерами їх не часто можна виявити і відповідно представити чіткий алгоритм виконання операцій аналізу вразливості. Мета роботи: розробити математичну модель технології тестування DOM XSS вразливостей для аналітичної оцінки часових витрат.

Виклад основного матеріалу.

Алгоритм виявлення комплексу DOM XSS вразливостей. Для математичної формалізації алгоритму виявлення комплексу DOM XSS вразливостей різних типів скористаємося основними положеннями мережевого GERT-моделювання, докладно описаними в роботах [7, 8].

Відповідно до алгоритму аналізу DOM XSS вразливості основні етапи можна описати таким чином:

1) З коду аналізованої сторінки витягуються всі теги <script> і формується список тегів для аналізу.

2) Виконується аналіз вмісту тега. При цьому, якщо теги не містять код, а посилаються на віддалений файл, виконується звернення до файлу та отримання коду з нього. У вмісті файлу знаходяться потенційні небезпечні ділянки коду (sink), які використовують вхідні дані клієнта (source).

3) Якщо в коді тега використовується source, виконується атака з певним маркером, який можна відстежити в DOM структурі сторінки після виконання коду (наприклад, ін'єкція певного текстового вмісту в DOM).

4) Виконується перевірка вмісту DOM. Якщо в результаті атаки маркер знаходиться в DOM, можна зробити висновок про наявність DOM вразливості.

5) Після впровадження даних вручну і аналізу результатів, виконуваності на перших 4 етапах виконується аудит коду (може бути здійснений дистанційно).

6) Кроки 2 – 5 виконуються для кожного тега script на сторінці.

Для побудови формальної моделі алгоритму виявлення комплексу DOM XSS вразливостей обрана стохастична GERT- мережу.

Проведені дослідження показали, що GERT (Graphical Evaluation and Review Technique) – є методом вивчення та аналізу стохастичних мереж, які використовуються для опису логічного взаємозв'язку між частинами проекту або етапами процесу [7]. Головною метою GERT є оцінка логіки мережі і тривалість активності і отримання висновку про необхідність виконання деяких активностей.

Мережі GERT складаються з вузлів типу AND, INCLUSIVE-OR і EXCLUSIVE-OR, і гілок з двома і більше параметрами. Гілка, має напрямок, має вузол початку і вузол кінця. Параметри гілки містять:

1) ймовірність проходження гілки (Pa) за умови, що вузол, який є джерелом гілки, був реалізований;

2) час (ta) проходження гілки, якщо вона буде реалізована.

Час ta може бути випадковою величиною. Якщо гілка не є частиною реалізації мережі, тобто під час виконання процесу активність, пов'язана з гілкою, не відбувається, то ta = 0.

Вузол в стохастичній мережі GERT складається з функції входу (контрибутивної функції) і функції виходу (дистрибутивної функції). Кожна з функцій описується певним логічним відношенням щодо пов'язаних гілок.

В цілому, проведені дослідження показали, що GERT-моделювання є ефективним способом визначення заздалегідь невідомих законів і функцій розподілу випадкових величин при відомому алгоритмі функціонування (процесу). Саме тому, як інструмент математичного моделювання, нами було вибрано GERT-моделювання.

GERT-модель технології тестування комплексу DOM XSS вразливостей. Побудуємо, відповідно до представленого описом мережеву GERT-модель технології тестування комплексу DOM XSS вразливостей. Графічне зображення GERT-моделі представлено на рис. 1

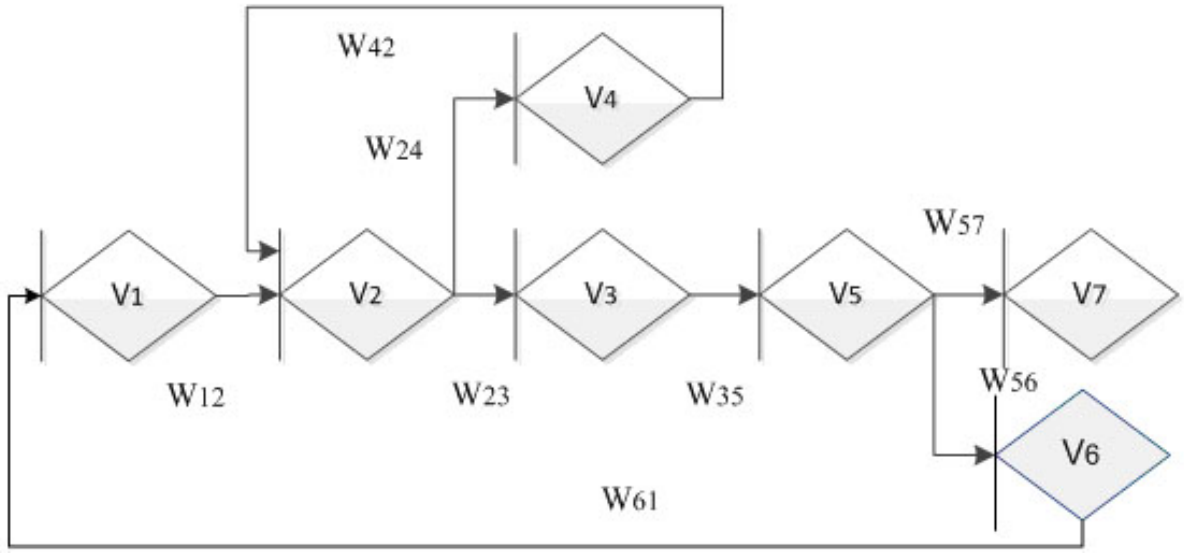

Рисунок 1 – GERT-модель технології тестування комплексу DOM XSS вразливостей
Джерело: розроблено автором

У представленій мережі вузли графа інтерпретуються станами комп'ютерної системи в процесі функціонування DOM структури, а гілки графа – ймовірносно-тимчасовими характеристиками переходів між станами. Зокрема гілка (1,2) описує процес отримання та аналізу вмісту тега. Гілка (2,3) відображає процес виконання атаки в разі наявності «Source» структури. Гілка (2,4) визначається процедурами звернення до вмісту віддаленого файлу (пошук «sink»). Гілка (4,2) характеризує повернення на виконання атаки. Гілка (3,5) описує продовження атаки, зокрема перевірку вмісту DOM. Гілка (5,6) характеризує одну з основних особливостей аналізу алгоритму XXS вразливостей різних типів – автоматичний аудит коду (при необхідності віддалений). Гілка (5,1) відображає процес переходу до нового тегу. Далі гілка (5,7) характеризує заключну стадію прийняття рішення про уразливість. Характеристики гілок моделі представлені в табл. 1.

Таблиця 1 – Характеристики гілок моделі

№ п/п	Гілка	W-функція	Ймовірність	Функція, що походить від моментів
1	(1,2)	W_{12}	p1	$\lambda_1/(\lambda_1 - s)$
2	(2,3)	W_{23}	p2	$\lambda_2/(\lambda_2 - s)$
3	(2,4)	W_{24}	p3	$\lambda_3/(\lambda_3 - s)$
4	(3,5)	W_{35}	p2	$\lambda_2/(\lambda_2 - s)$
5	(5,6)	W_{56}	p4	$\lambda_4/(\lambda_4 - s)$
6	(6,1)	W_{51}	1 – p4	$\lambda_5/(\lambda_5 - s)$
7	(4,2)	W_{42}	p3	$\lambda_3/(\lambda_3 - s)$
8	(5,7)	W42	p4	$\lambda_4/(\lambda_4 - s)$

Джерело: розроблено автором

Особливість даного процесу полягає в різнорідності аналізованих і оброблюваних даних. При цьому можливі різні випадки організації зворотного зв'язку. На рис. 1 ці цикли зафіксовані у вигляді переходів $W_{12} \to W_{24} \to W_{42}$, $W_{12} \to W_{23} \to W_{35} \to W_{56} \to W_{61}$.

Еквівалентна W-функція часу виконання алгоритму тестування комплексу DOM XSS різних типів (в тому числі DOM Based XSS) вразливостей дорівнює:

$$W_E(s) = \frac{W_{12}W_{23}W_{35}W_{56} + W_{12}W_{24}W_{42}W_{23}W_{35}W_{57}}{1 - W_{12}W_{23}W_{35}W_{51} - W_{12}W_{24}W_{42}W_{23}W_{35}W_{56}W_{61}} =$$

$$= \frac{p_1 p_2^2 \lambda_1 \lambda_2^2 \left(p_4 \lambda_4 (\lambda_3 - s)^2 (\lambda_5 - s) + p_3^2 q_1 \lambda_3^2 \lambda_5 (\lambda_4 - s)\right)}{(\lambda_4 - s)\begin{pmatrix}(\lambda_1 - s)(\lambda_2 - s)^2 (\lambda_3 - s)^2 (\lambda_5 - s) - \\ - p_1 \lambda_1 p_2^2 \lambda_2^2 q_1 \lambda_5 (\lambda_3 - s)^2 - p_1 p_2^2 p_3^2 p_4 \lambda_1 \lambda_2^2 q_1 \lambda_3^2 \lambda_4 \lambda_5\end{pmatrix}}, \quad (1)$$

де $1 - p_4 = q_1$.

Для GERT-мереж з циклами не існує простих методів знаходження особливих точок функції $\Phi_E(z)$заміни дійсних змінних $(z = -i\varsigma)$, де ς- дійсна змінна. Це пояснюється тим, що для знаходження особливих точок необхідно вирішувати нелінійні рівняння, і чим складніше структура GERT-мережі, тим складніше і вихідне рівняння. Тому в ході моделювання пропонується вдатися до подібної заміни.

Виконуючи комплексне перетворення $z = -s$, отримаємо:

$$\Phi(z) = \frac{uz^3 + vz^2 + bz + k}{(\lambda_4 + z)\left(z^6 + cz^5 + dz^4 + gz^3 + hz^2 + wz + m\right)}, \quad (2)$$

де

$u = -p_1 p_2^2 p_4 \lambda_1 \lambda_2^2 \lambda_4$,

$v = p_1 p_2^2 p_4 \lambda_1 \lambda_2^2 \lambda_4 (\lambda_5 + 2\lambda_3)$,

$b = -p_1 p_2^2 p_4 \lambda_1 \lambda_2^2 \lambda_4 \lambda_3 (2\lambda_5 - \lambda_3)$,

$k = -p_1 p_2^2 \lambda_1 \lambda_2^2 \lambda_3^2 \lambda_4 \lambda_5 (p_4 + p_3^2 q_1)$,

$c = \lambda_1 + 2\lambda_2 + 2\lambda_3 + \lambda_4 + \lambda_5$,

$d = -(2\lambda_3\lambda_5\lambda_4 + \lambda_1\lambda_5\lambda_4 + 2\lambda_2\lambda_5\lambda_4 + \lambda_3^2 + 2\lambda_1\lambda_3 + 4\lambda_2\lambda_3 + 2\lambda_1\lambda_2 + \lambda_2^2)$,

$g = \begin{pmatrix}\lambda_3^2\lambda_4\lambda_5 + 4\lambda_1\lambda_2\lambda_4\lambda_5 + 4\lambda_2\lambda_3\lambda_4\lambda_5 + \lambda_2^2 + \lambda_3^2\lambda_1 + 2\lambda_3^2\lambda_2 + 4\lambda_1\lambda_2\lambda_3\lambda_4 + \\ + 2\lambda_2^2\lambda_3 + \lambda_2^2\lambda_1 + \lambda_3^2\lambda_4 + \lambda_2^2\lambda_4\end{pmatrix}$,

$h = -\begin{pmatrix}\lambda_1\lambda_3^2\lambda_4\lambda_5 + 2\lambda_2\lambda_3^2\lambda_4\lambda_5 + 4\lambda_1\lambda_2\lambda_3\lambda_4\lambda_5 + 2\lambda_2^2\lambda_3\lambda_4\lambda_5 + \lambda_2^2\lambda_3^2\lambda_4 + \\ + 2\lambda_1\lambda_2^2\lambda_3\lambda_4 - p_1 p_2^2 p\ q_1\lambda_1\lambda_2\lambda_4\lambda_5\end{pmatrix}$,

$w = \lambda_1\lambda_2\lambda_3^2\lambda_4\lambda_5 + \lambda_2^2\lambda_3^2\lambda_4\lambda_5 + 2\lambda_1\lambda_2^2\lambda_3\lambda_4\lambda_5 + \lambda_1\lambda_2^2\lambda_4\lambda_3 - 2p_1p_2^2p_4q_1\lambda_1\lambda_2\lambda_3\lambda_4\lambda_5$,

$m = p_1 p_2^2 p_4 q_1 \lambda_1 \lambda_2 \lambda_3^2 \lambda_4 \lambda_5 + p_1 p_2^2 p_3 p_4 q_1 \lambda_1 \lambda_2^2 \lambda_3^2 \lambda_4 \lambda_5 - \lambda_1 \lambda_2^2 \lambda_3 \lambda_4 \lambda_5$.

Щільність розподілу ймовірностей часу виконання алгоритму аналізу DOM XSS вразливості:

$$\varphi(x)=\frac{1}{2\pi i}\int_{-i\infty}^{i\infty}e^{zx}\frac{\mathrm{u}z^3+vz^2+bz+k}{\left(z^6+cz^5+dz^4+gz^3+hz^2+wz+m\right)}dz, \tag{3}$$

де операція інтегрування виконується за допомогою інтеграла Бромвіча-Вагнера [8].

Спосіб інтегрування залежить від того, чи має функція Φ(z) тільки прості полюси, або полюси деякого порядку. У тому випадку, коли функція Φ(z) має тільки прості полюси, вираз $e^{zx}\Phi(z)$ можна представити у вигляді:

$$e^{zx}\Phi(z)=\frac{e^{zx}\left(\mathrm{u}z^3+vz^2+bz+k\right)}{z^7+\gamma_6z^6+\gamma_5z^5+\gamma_4z^4+\gamma_3z^3+\gamma_2z^2+\gamma_1z+\gamma_0}=\frac{\mu(z)}{\psi(z)}, \tag{4}$$

де $\gamma_6=c$, $\gamma_5=c+d$, $\gamma_4=d+g$, $\gamma_3=g+h$, $\gamma_2=h+w$, $\gamma_1=w+m$, $\gamma_0=m$.

Тоді щільність розподілу часу виконання алгоритму аналізу DOM XSS вразливості всіх типів дорівнює:

$$\begin{aligned}\varphi(x)&=\sum_{k=1}^{7}\mathrm{Re}\,s\left[e^{zx}\Phi(z)\right]=\sum_{k=1}^{7}\frac{\mu(z_k)}{\psi(z_k)}=\\&=\sum_{k=1}^{7}\frac{e^{zx}\left(\mathrm{u}z^3+vz^2+bz+k\right)}{7z_k^6+6\gamma_6z_k^5+5\gamma_5z_k^4+4\gamma_4z_k^3+3\gamma_3z_k^2+2\gamma_2z_k+\gamma_1}.\end{aligned} \tag{5}$$

Функція $\Phi(z)$ крім рішень, які визначаються коренями рівняння $z^6+cz^5+dz^4+gz^3+hz^2+wz+m=0$, може мати і полюс другого або третього порядку. Тоді щільність розподілу часу передачі повідомлення $\varphi(x)$ знаходиться за формулою знаходження відрахувань r_{-1} від полюсів z_k порядку n:

$$r_{-1}=\frac{1}{(n-1)!}\lim_{z\to z_k}\frac{d^{n-1}\left((z-z_k)^ne^{zx}\Phi(z)\right)}{dz^{n-1}}. \tag{6}$$

Вираз (6) являє собою дрібно-раціональну функцію щодо z зі ступенем знаменника більшою, ніж ступінь чисельника. Тому для нього виконується умови леми Жордана [9].

Багаточлен $\mathrm{z}^6+\mathrm{cz}^5+\mathrm{dz}^4+\mathrm{gz}^3+\mathrm{hz}^2+\mathrm{wz}+\mathrm{m}$ породжує сім полюсів. Вирішення рівняння:

$$z^6+cz^5+dz^4+gz^3+hz^2+wz+m=0 \tag{7}$$

може бути знайдено будь-яким методом, наприклад, за формулами Вієта [10]. В результаті обчислюються особливі точки z_1, z_2, z_3, z_4, z_5, z_6.

Таким чином, на основі експоненційної GERT-мережі розроблено математичну модель технології тестування комплексу DOM XSS вразливостей всіх типів («stored XSS», «reflected XSS» і DOM Based XSS), яка відрізняється від відомих, урахуванням їх специфіки та необхідності автоматичного аудиту DOM Based XSS окремо.

Розроблена модель може бути використана для дослідження інтернет Web-застосунків в мережевих структурах, а також при розробці нових засобів і протоколів захисту даних в комп'ютерних системах і мережах.

Застосування експоненційних стохастичних моделей GERT дасть можливість використання результатів, отриманих в аналітичному вигляді (функції, щільності

розподілу) для проведення порівняльного аналізу і досліджень, більш складних комп'ютерних систем математичними методами.

Висновки. У роботі розроблена математична модель процесу тестування Web-застосунків. В основу математичного моделювання покладено підхід GERT-мережевого синтезу. В результаті розроблено математичні моделі технології тестування DOM XSS вразливості.

Математична модель технології тестування комплексу DOM XSS вразливостей відрізняється від відомих, урахуванням специфіки комплексного аналізу різних типів XSS вразливості («stored XSS», «reflected XSS» і DOM Based XSS), а також включенням в алгоритм процедур автоматичного аудиту DOM Based XSS окремо. Це дає можливість провести аналітичну оцінку тимчасових витрат тестування зазначених вразливостей в умовах реалізації стратегії розробки безпечного програмного забезпечення.

Список літератури

1. About The Open Web Application Security Project – OWASP. URL: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project (Last accessed: 08.12.2019)
2. Смирнов А.А. , Коваленко А.В., Якименко Н.Н., Доренский А.П. Проблемы анализа и оценки рисков информационной деятельности. *Системи обробки інформації: збірник наукових праць*. 2016. Вип. 3(140). С. 40-42.
3. Смирнов А.А., Коваленко А.В. Методы качественного анализа и количественной оценки рисков разработки программного обеспечения. *Системи обробки інформації: збірник наукових праць*. 2016. Вип. 5(142). С. 153-157.
4. Коваленко А.В. Метод управления рисками разработки программного обеспечения. *Системи управління, навігації та зв'язку*. 2016. Вип. 2 (38). С. 93-100.
5. OSSTMM 3 – The Open Source Security Testing Methodology Manual. Contemporary Security Testing And Analysis. URL: http://www.isecom.org/mirror/OSSTMM.3.pdf (Last accessed: 10.12.2019)
6. Positive Research 2016. URL: https://www.ptsecurity.com/upload/ptru/analytics/Positive-Research-2016-rus.pdf (Last accessed: 08.12.2019)
7. Semenov S.G., Zmiyevskaya V N., Kassem Khalife Development of Gert model of management system by using test cases. *Journal of Qafqaz university-mathematics and computer science.* 2016. Vol.(4), № 1. С. 52-59.
8. Testing for DOM-based Cross-site scripting (OTG-CLIENT-001) – OWASP. URL: https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001) (Last accessed: 08.12.2019)
9. Cohen W., Ravikumar P., Fienberg S. A Comparison of String Metrics for Matching Names and Records. URL: https://www.cs.cmu.edu/afs/cs/Web/People/wcohen/postscript/kdd-2003-match-ws.pdf (Last accessed: 11.12.2019)
10. Kevin Dressler, Axel-Cyrille Ngonga Ngomo. On the Efficient Execution of Bounded Jaro-Winkler Distances. *Semantic Web* – Interoperability, Usability, Applicability an IOS Press Journal. URL: http://www.semantic-web-journal.net/system/files/swj944.pdf (Last accessed:6.12.2019)

References

1. About The Open Web Application Security Project – OWASP. *www.owasp.org*. Retrieved from: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project.
2. Smirnov, A.A., Kovalenko, A.V., Jakimenko, N.N. & Dorenskij, A.P. (2016). Problemy analiza i ocenki riskov informacionnoj dejatel'nosti [Problems analysis and risk assessment information activities]. *Sistemi obrobki informacii – Information Processing Systems*, *Vol. 3(140),* 40-42 [in Russian].
3. Smirnov, A.A. & Kovalenko, A.V. (2016). Metody kachestvennogo analiza i kolichestvennoj ocenki riskov razrabotki programmnogo obespechenija [Methods of qualitative analysis and quantitative risk assessment software development]. *Sistemi obrobki informacii – Information Processing Systems*, *Vol. 5(142),* 153-157 [in Russian].

4. Kovalenko, A.V. (2106). Metod upravlenija riskami razrabotki programmnogo obespechenija [Software Development Risk Management Method]. *Sistemi upravlinnja, navigacii ta zv'jazku – Control, Navigation and Communication Systems . Vol. 2 (38)*. S. 93-100 [in Russian].
5. OSSTMM 3 – The Open Source Security Testing Methodology Manual. Contemporary Security Testing And Analysis. *www.isecom.org*. Retrieved from: http://www.isecom.org/mirror/OSSTMM.3.pdf.
6. Positive Research 2016: Retrieved from: https://www.ptsecurity.com/upload/ptru/analytics/Positive-Research-2016-rus.pdf.
7. Semenov, S.G., Zmiyevskaya, V N. & Kassem, Khalife (2016). Development of Gert model of management system by using test cases. *Journal of Qafqaz university-mathematics and computer science*, *Vol.(4), 1*, 52-59
8. Testing for DOM-based Cross-site scripting (OTG-CLIENT-001) – OWASP: Retrieved from: https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001).
9. Cohen W., Ravikumar P., Fienberg S. A Comparison of String Metrics for Matching Names and Records William W. Cohen, Pradeep Ravikumar, Stephen E. Fienberg. Retrieved from: https://www.cs.cmu.edu/afs/cs/Web/People/wcohen/postscript/kdd-2003-match-ws.pdf.
10. Kevin Dressler & Axel-Cyrille Ngonga Ngomo. (2015). On the Efficient Execution of Bounded Jaro-Winkler Distances / Semantic Web – Interoperability, Usability, Applicability an IOS Press Journal. Retrieved from: http://www.semantic-web-journal.net/system/files/swj944.pdf

Oleksandr Kovalenko, Assoc. Prof., PhD tech. sci**.**
Central Ukrainian National Technical University, Kropyvnytskyi, Ukraine

Mathematical Model of DOM XSS Vulnerability Testing Technology for Analytical Assessment of Time Costs

The paper presents the results of the study and testing algorithms for vulnerability to one of the most common types of attacks on Web applications, DOM XSS, for analytic assessment of time costs. Analysis of various kinds of statistical materials of well-known organizations (for example, the Open Web Application Security Project) showed that one of the most dangerous types of attacks (vulnerabilities) is Cross Site Scripting – XSS. In a number of works, attempts of mathematical formalization the process of finding and eliminating vulnerabilities of this kind were made . However, the presented models do not take into account the latest trends of XSS vulnerability, namely the difference in their types ("stored XSS", "reflected XSS" and DOM Based XSS) and the need to identify them. That is why a particularly relevant task in this direction seems to be the modeling of the DOM (Document Object Model) XSS vulnerability algorithm taking into account the complex of their three possible types.

In general, studies have shown that GERT-modeling is an effective way to determine previously unknown laws and distribution functions of random variables with a known algorithm of functioning (process). That is why, we chose GERT modeling as a tool for mathematical modeling. The main purpose of GERT is to evaluate the network logic and the duration of the activity and obtaining a conclusion on the need to perform certain activities.

As a result, a mathematical model was developed for testing the DOM XSS vulnerability complex which differs from the known ones by taking into account the specifics of complex analysis of various types of XSS vulnerability ("stored XSS", "reflected XSS" and DOM Based XSS), as well as separately including DOM Based XSS into the algorythm of automatic audit procedures. This makes it possible to conduct an analytical assessment of the time spent testing these vulnerabilities in the context of implementing a secure software development strategy.

testing technologies, DOM XSS vulnerabilities, GERT modeling, security vulnerabilities

Одержано (Received) .17.12.2019 *Прорецензовано (Reviewed) 20.12.2019*
Прийнято до друку (Approved) 23.12.2019