Вісник ЛДУБЖД

Bulletin of Lviv State University of Life Safety

ISSN 2078-4643 (print), ISSN 2708-1389 (online)
https://journal.ldubgd.edu.ua/index.php/Visnuk/
УДК 004.056.53: 004.491: 004.492
DOI: 10.32447/20784643.22.2020.03

М.-В. М. Либа, Л.Є. Угрин
Національний університет «Львівська політехніка»

СУЧАСНІ ІНСТРУМЕНТИ ТЕСТУВАННЯ БЕЗПЕКИ OWASP

Анотація. Із розвитком інформаційних технологій людство все більше заглиблюється у світ гаджетів, хмарних технологій, віртуальної реальності і штучного інтелекту. Через web-додатки отримуємо і поширюємо інформацію, в тому числі і конфіденційну. Під час пандемії велика частина людей перейшла в онлайн режим роботи і навчання. В результаті, більшість даних, які зберігаються на персональних комп'ютерах, серверах компаній, хмарних сховищах, потребують захисту від кібератак. Проблема кібербезпеки на цей час неймовірно актуальна через зламування криптобірж, сайтів міністерств, біткоїн-гаманців чи акаунтів соцмереж. Для забезпечення надійного захисту різної інформації потрібно проводити якісне тестування розроблених додатків на виявлення кіберзагроз. В статті зазначено, що при тестуванні додатків виконується перевірка на вразливості, які могли б виникнути в результаті неправильного налаштування системи або через недоліки програмних продуктів. Важливим є питання використання інновацій для покращення якості, зокрема сучасні реалії стали викликом для розвитку продуктів забезпечення кібербезпеки. Розвиток технологій вимагає від сучасних компаній оновлення своїх IT систем і проведення регулярних перевірок безпеки. Дослідження в роботі присвячене аналізу сучасних інструментів тестування OWASP, які сприяють забезпеченню безпеки даних, з метою їх подальшого використання. Open Web Application Security Project є відкритим проєктом забезпечення безпеки. При дослідженнях виявлено список найбільш небезпечних векторів атак на Web-додатки, зокрема OWASP ZAP здійснює сканування безпеки системи на базовому рівні шляхом аналізу надісланих та отриманих даних, а тестування безпеки мобільних додатків та мобільних пристроїв iOS та Android здійснюється за MSTG. Практичним результатом роботи є проведення тестування спеціально розробленого web-додатку і виявлення вразливостей різного рівня критичності.

Ключові слова: тестування, вразливість, безпека, IT-технології, OWASP.

M.-V. M. Lyba, L. E. Uhryn
Lviv Polytechnic National University

MODERN TOOLS FOR SECURITY TESTING FROM OWASP

With the development of information technology, humanity is increasingly delving into the world of gadgets, cloud technology, virtual reality, and artificial intelligence. Through web applications, we receive and distribute information, including confidential. During the pandemic, most people switched to online work and study. As a result, most of the data stored on personal computers, company servers, and cloud storage needs protection from cyberattacks. The problem of cybersecurity at the moment is incredibly relevant due to the hacking of cryptocurrencies, websites of ministries, bitcoin wallets or social network accounts. It is necessary to conduct high-quality testing of developed applications to detect cyber threats, to ensure reliable protection of different information. The article states that when testing applications, it checks for vulnerabilities that could arise as a result of incorrect system setup or due to shortcomings in software products. The use of innovation is necessary to improve quality. Modern realities have become a challenge for the development of cybersecurity products. Improvement of technology requires modern companies to update their IT systems and conduct regular security audits. The research is devoted to the analysis of modern OWASP testing tools that contribute to data security, with a view to their further use. The Open Web Application Security Project is an open security project. The research revealed a list of the most dangerous vectors of attacks on Web-applications, in particular, OWASP ZAP performs analyzes the sent and received data system security scanning at the primary level, MSTG performs security testing of mobile applications iOS and Android mobile devices. The practical result of the work is to test a specially developed web-application and identify vulnerabilities of different levels of criticality.

Keywords: testing, vulnerability, safety, IT technologies, OWASP.

Вступ

Сучасний світ несе в собі тисячі загроз і потенційних небезпек. Всесвітня мережа, що стала невід'ємною частиною нашого життя, не є винятком. Кіберзлочинність зараз розвинена як ніколи

- адже майже кожна компанія має свій сайт в Інтернеті, а зловмисник у мережі може легко залишатися абсолютно анонімним. Надзвичайно актуальною темою на сьогодні є тема захисту web-додатків від потенційних атак ззовні, оскільки разом з новими методами розробки, виникають і нові методи атак [1].

Також необхідно відзначити різні сучасні світові проекти із захисту від атак на web-додатки. Зокрема, для допомоги фірмам формулювати та впроваджувати системи безпеки для різних додатків і реакції на бізнес-ризики використовується модель зрілості із забезпечення впевненості у програмному забезпеченні (SAMM). Існують також різноманітні настанови стосовно коду, тестування та розробки для забезпечення безпеки web-додатків, що містять низькорівневе тестування на проникнення із забезпеченням необхідного рівня конфіденційності [2]. Дуже важливою є настанова із реагування на топ-десять інцидентів безпеки, яку можуть використовувати інженери з безпеки, аудитори, юристи, правоохоронці та розробники додатків. Також існує проєкт захисту від Proxy атак (ZAP), який можуть використовувати при тестуванні на проникнення. Важливо зазначити, що для захисту розробляються тестові небезпечні web-додатки для навчання безпечним методам програмування, наприклад Webgoat.

Методи досліджень

OWASP (Open Web Application Security Project) – відкритий проєкт забезпечення безпеки web-додатків. Спільнота OWASP включає в себе корпорації, освітні організації і приватні особи з усього світу. Спільнота працює над створенням статей, навчальних посібників, документації, інструментів і технологій, які перебувають у вільному доступі. Фонд OWASP це благодійна організація, яка надає підтримку і здійснює управління проектами та інфраструктурою OWASP. Продукти OWASP використані при тестуванні:

- OWASP Top 10;
- OWASP Top 10 Privacy Risks Project;
- OWASP Zed Application Proxy (ZAP);
- OWASP Web Security Testing Guide (WSTG);
- OWASP Application Security Verification Standard (ASVS);
- OWASP Juice Shop.

OWASP створив список з 10-ти найбільш небезпечних векторів атак на Web-додатки в якому зосереджені найнебезпечніші вразливості, які можуть коштувати деяким людям великих грошей, або підриву ділової репутації, аж до втрати бізнесу. OWASP TOP-10 не є офіційним стандартом, це лише інформаційний документ, який широко використовується багатьма організаціями, програмами виплати винагород за виявлені вразливості і експертами в області кібербезпеки для класифікації рівня небезпеки вразливостей. Верхній рядок TOP-10 займають вразливості, що дозволяють впровадження коду.

За останні роки рейтинг оновлювався декілька разів – в 2013 і 2017 роках. Проте в новій версії відбулися перестановки, а також додалися три нові типи вразливостей: XXE (External Entity Expansion, вразливість сайту або додатка до впровадження коду XML), Insecure Deserialization і Insufficient Logging & Monitoring [3].

Результати досліджень

OWASP Top 10 Privacy Risks Project містить 10 ризиків конфіденційності у web-програмах. Він охоплює технологічні та організаційні аспекти, які зосереджені на реальних ризиках, а не лише на юридичних питаннях. Проєкт надає поради щодо впровадження конфіденційності шляхом дизайну у web-додатки з метою допомогти розробникам та постачальникам краще зрозуміти та покращити конфіденційність. Список використовує рекомендації OECP, а також може бути використаний для оцінки ризиків конфіденційності, пов'язаних із конкретними web-програмами.

Вразливість є ключовою проблемою будь якої системи. Неможливість належним чином розробити та впровадити додаток, виявити проблему або негайно застосувати виправлення призводить до порушення конфіденційності. Web Application Vulnerabilities – захищає або оперує конфіденційними даними користувачів.

Operator-sided Data Leakage застосовують через неможливість запобігти витоку будь-якої інформації, що містить або пов'язана з даними користувача, що призводить до втрати конфіденційності даних через навмисне порушення, або через ненавмисну помилку, наприклад, спричинену недостатнім контролем доступу, ненадійним зберіганням, дублюванням даних або недостатньою обізнаністю.

Insufficient Data Breach Response – оцінка ризиків через те, що постраждалі особи не мають інформації про можливе порушення або витік даних, спричинене умисними або ненавмисними подіями через ситуацію, коли не обмежують доступ до даних.

Оскільки не завжди є достатньо інформації для опису обробки даних та місця їх зберігання, то Insufficient Deletion of personal data дає змогу унеможливити видалення персональних дані після припинення зазначеної дії або після закінчення дії запиту.

Non-transparent Policies, Terms and Conditions унеможливлює зробити персональну інформацію легкодоступною. Існують ризики порушення конфіденційності при зборі описових,

демографічних чи будь яких інших даних, пов'язаних з користувачами.

Collection of data not required for the primary purpose застосовується до оцінки даних, на які користувач не дав згоди.

Sharing of data with third party тестує ризики надання даних користувача третій стороні без отримання згоди користувача. Обмін даними може відбутися через неналежне використання сторонніх ресурсів web-сайту, таких як віджети, аналітика або web-помилки.

Outdated personal data застосовують коли використовують застарілі, неправильні або неправдивих дані користувачів, Missing or Insufficient Session Expiration – коли неможливо ефективно забезпечити припинення сеансу і це може призвести до збору додаткових даних без згоди або обізнаності користувача.

Якщо неможливо забезпечити передачу даних за зашифрованими та захищеними каналами, включаючи можливість витоку даних, то оцінка проводиться Insecure Data Transfer.

OWASP ZAP є безкоштовним і простим у використанні сканером, дозволяє здійснити сканування безпеки системи на базовому рівні шляхом аналізу надісланих та отриманих даних. Даний сканер добре підходить для початку вивчення основ тестування безпеки, але він також є і хорошим доповненням при тестуванні безпеки висококласними фахівцями[4]. Основними можливостями тестування цього сканера є:

- тестування на XSS атаки;
- тестування на можливість SQL-ін'єкцій;
- тестування додатка методом Fuzzing;
- контроль мережевих протоколів;
- складання звітів за результатами тестування.

Сканер надає можливість використання активного і пасивного методів сканування. Активний метод полягає в імітації дій зловмисника і безпосередній спробі проникнення і зламу системи. Пасивний метод дає змогу проводити тестування на основі аналізу відправлених і прийнятих пакетів під час ручного тестування Security Testing інженера.

Проєкт OWASP Application Security Verification Standard (ASVS) забезпечує основу для тестування технічних засобів контролю безпеки web-додатків, а також надає розробникам список вимог до безпеки розробки [5]. Основною метою цього проєкту є нормалізація діапазону охоплення і рівня жорсткості, доступних на ринку, коли справа доходить до виконання перевірки безпеки web-додатків за допомогою комерційно-працюючого відкритого стандарту. Стандарт надає основу для тестування технічних засобів контролю безпеки додатків, а також будь яких технічних засобів контролю безпеки в середовищі, на яке опираються для захисту від таких вразливостей, як міжсайтовий скриптинг (Cross-Site Scripting, XSS) і SQL-ін'єкції. Цей стандарт може бути використаний для встановлення рівня довіри до безпеки web-додатків. Вимоги були розроблені з врахуванням таких цілей:

- використання в якості метрики - надання розробникам додатків і власникам додатків мітки, за допомогою якої можна оцінити ступінь довіри;
- використання в якості інструкції – надання інструкції для розробників засобів контролю безпеки щодо вживлення безпекової складової в додатки;
- використання під час закупівлі – забезпечення основи для вказівки в контрактах вимог щодо перевірки безпеки додатків.

Нові технології завжди створюють нові ризики для безпеки і мобільні додатки не є винятком. Проблеми безпеки мобільних додатків дещо відрізняються від традиційного настільного програмного забезпечення. Сучасні мобільні операційні системи, мабуть, більш безпечні, ніж настільні операційні системи, але проблеми також виникають, якщо ретельно не розглянуто питання безпеки під час розробки. Зберігання даних, зв'язок між програмами, належне використання криптографічних API та безпечне мережеве спілкування – лише деякі аспекти, які потрібно врахувати. Багато тестувальників безпеки мобільних додатків мають досвід тестування на проникнення в мережі та web-додатки, що є великою цінністю. Майже кожен мобільний додаток розмовляє із серверною сервісною службою і ці служби схильні до тих самих типів атак, які нам відомі у web-програмах на настільних машинах. Мобільні програми відрізняються тим, що там менша поверхня атак і, отже, більший захист від ін'єкцій та подібних атак. Натомість ми повинні визначити пріоритет захисту даних на пристрої та в мережі для підвищення мобільної безпеки.

MSTG – це повний посібник для тестування безпеки мобільних додатків та інженерного зворотного проєктування для тестувальників мобільних пристроїв iOS та Android, у якому можна знайти інформацію про внутрішні пристрої мобільної платформи; тестування безпеки в життєвому циклі розробки мобільних додатків; основні статичні та динамічні тестування безпеки; зворотне проєктування та фальсифікація мобільних додатків; оцінка захисту додатку; детальні тестові приклади, що відповідають вимогам MASVS [6].

MASVS (Mobile AppSec Verification Standard) визначає модель безпеки мобільних додатків та перераховує загальні вимоги безпеки для

мобільних додатків [7]. Його можуть використовувати архітектори, розробники, тестувальники, фахівці з безпеки та споживачі для визначення якостей безпечного мобільного додатка. MSTG відповідає одному і тому ж базовому набору вимог безпеки, пропонованих MASVS, і залежно від контексту вони можуть використовуватися як окремо, так і комбіновано для досягнення різних цілей.

Вимоги MASVS можна використати на етапах планування та проєктування архітектури програми, тоді як контрольний список та посібник з тестування можуть служити основною базою для ручного тестування безпеки або як шаблон для автоматизованих тестів безпеки.

WSTG (Web Security Testing Guide) є комплексною інструкцією з тестування безпеки web-додатків і web-сервісів, яка використовується пентестерами і організаціями по всьому світу [8]. Актуальною є версія - [Version 4.1] - 2020-04-2, попередня версія - [Version 4.0] - 2014-09-17 – між оновленнями минуло близько 6 років, що охоплює великий пласт сучасних технологій, однак фундаментальні зміни чекатимуть тільки в 5 версії WSTG.

Оскільки OWASP Top 10 дає знання щодо найрозповсюдженіших вразливостей, OWASP ZAP безкоштовний та потужний інструмент для тестування та Web Security Testing Guide покрокова інструкція з тестування, яка покриває всі можливі області web-сервісу, то це дозволяє OWASP Web Security Testing Guide цими засобами успішно тестувати web-додатки.

Хоча це вузьконаправлене програмне забезпечення для тестування безпеки та пройшовши практичний курс з застосуванням отриманих навичок можна самостійно тестувати web-додатки, що надзвичайно актуально сьогодні.

За допомогою інструментів наведених вище, було проведено тестування іншого продукту OWASP – OWASP Juice Shop [9]. Це спеціально розроблений web-додаток, який має наперед передбачені вразливості, що допомагає закріпити на практиці теоретичні знання вразливостей і те. яким чином їх виявляти.

Під час тестування було виявлено 15 вразливостей різного рівня критичності, зокрема 3 критичних вразливості, 3 високої критичності, 5 середньої критичності, 2 низької критичності та 2 інформаційних попередження. В кінці тестування був складений звіт щодо виявлених вразливостей, де було показано всі кроки з відтворення та надані рекомендації стосовно того, як виправити вразливість (рис. 1).

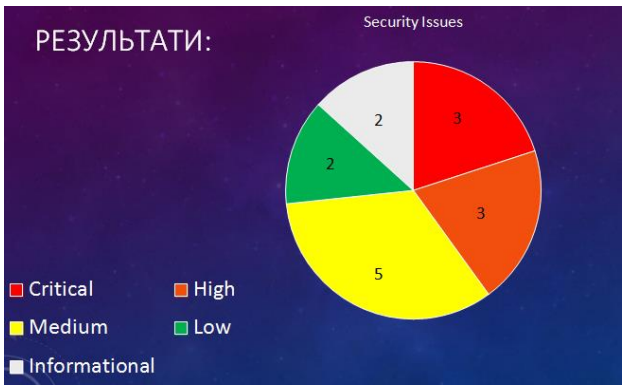

Рисунок 1 – Результати тестування

Обговорення результатів досліджень

З проведених досліджень випливає, що OWASP продукти доцільно використовувати для тестування безпеки. Провівши тестування на XSS атаки, тестування на можливість SQL-ін'єкцій, контроль мережевих протоколів, складається звіт вразливостей. Відповідно, оволодівши OWASP продуктами можна самостійно отримати теоретичні та практичні навички тестування безпеки web-додатків.

Висновки

В статті проаналізовано основні загрози безпеки в Інтернет і наведено рекомендації стосовно використання відкритого проєкту забезпечення безпеки web-додатків OWASP. Тестування одного із продуктів захисту OWASP Juice Shop дає змогу виявити проникнення в інформаційні системи, що підвищить конфіденційність інформації різних організацій.

Література:

1. Денисюк В.О. Захист інформації у локальних мережах. Вінниця: ВНАУ, 2017. С.55-56.

2. Скембрейц Дж. Безопасность Web-приложений - готовые решения. М.: Издательский дом «Вильямс», 2003. 384 с.

3. OWASP Top Ten. URL: https://owasp.org/www-project-top-ten/.

4. OWASP ZAP. URL: https://owasp.org/www-project-zap/.

5. OWASP ASVS. URL: https://owasp.org/www-project-application-security-verification-standard/

6. OWASP MSTG. URL: https://owasp.org/www-project-mobile-security-testing-guide/

7. OWASP MASVS. URL: https://github.com/OWASP/owasp-masvs

8. WSTG - v4.1. URL: https://owasp.org/www-project-web-security-testing-guide/v41/.

9. OWASP Juice Shop. URL: https://owasp.org/www-project-juice-shop/

References:

1. Denisyuk V.O. Zakhist information at local fences. Vinnytsya: VNAU, 2017. Pp. 55-56.
2. Skembreyts J. Security of Web-applications - ready-made solutions. M.: Publishing house "Williams", 2003. 384 p.
3. OWASP Top Ten. URL: https://owasp.org/www-project-top-ten/ (access October, 10, 2020).
4. OWASP ZAP. URL: https://owasp.org/www-project-zap/ (access July, 2, 2020).
5. OWASP ASVS. URL: https://owasp.org/www-project-application-security-verification-standard/ (access September, 11, 2020).
6. OWASP MSTG. URL: https://owasp.org/www-project-mobile-security-testing-guide/ (access October, 5, 2020).
7. OWASP MASVS. URL: https://github.com/OWASP/owasp-masvs (access May, 30, 2020).
8. WSTG - v4.1. URL: https://owasp.org/www-project-web-security-testing-guide/v41/ (access June, 9, 2020).
9. OWASP Juice Shop. URL: https://owasp.org/www-project-juice-shop/ (access October, 17, 2020).

*** Науково-методична стаття**