УДК 621.324

С.М. Порошин, О.О. Можаєв, М.О. Можаєв

Національний технічний університет «ХПІ», Харків

МЕТОДОЛОГІЯ ПРОВЕДЕННЯ PEN-ТЕСТУВАННЯ ВЕБ-ДОДАТКІВ

Проаналізовано основні підходи щодо проведення тестування на вразливості інформаційно-телекомунікаційних та комп'ютерних систем, зроблено вибір напряму pen-тестування веб-ресурсів. Згідно методології OWASP TOP 10 розроблено сценарії збору інформації, аналізу інформації та перевірки сайту. Визначено поширені помилки і уразливості. На основі статистичних даних основних небезпек веб-сайту розроблено варіант методології тестування веб-додатку. Зроблено висновок, що подальші розробки в цьому напрямі повинні вестися в площині класифікації, аналізу та управління окремими рівнями OWASP, розширення і врахування можливих кібератак на веб-ресурси.

Ключові слова: *pen-тестування, веб-додатки, сайт, кібер-атаки, хакерські зломи, Open Web Application Security Project.*

Вступ

Аналіз літератури та постановка завдання. Сучасні інформаційно-телекомунікаційні та комп'ютерні системи (ІТКС) є модульним і відкритим структурами. З одного боку це дозволяє динамічно розвиватися різним інформаційним і мережним технологіям, а з іншого надає базу знань для проведення злочинних дій хакерам.

На даний час одним з найбільш дієвих способів протидії зловмисним атакам на ІТКМ є впровадження механізмів попередження вторгнень. Одним з таких механізмів є система тестування на проникнення зловмисників (pen-тестування).

Аналіз літератури [1-7] показав, що pen-тест системи на стійкість до незаконного злому є досить ефективним і інформативним методом для оцінювання рівня захищеності комп'ютерної системи, а також локальної мережі, симулюючи хакерську спрямовану атаку.

Його метою виступає виявлення найбільш уразливих місць систем, що нерідко з'являються в результаті неправильного її налаштування. Також при допущених програмних і технічних помилках і внаслідок операційних недоліків, які часто можуть виникати при роботі.

Проведені дослідження показали, що pen-тестування складається з розширеного і поліпшеного практично списку перевірок наведених в міжнародних методиках:

- "Open Source Security Testing Methodology Manual" – Institute for Security and Open Methodologies (ISOM);
- "Guide for Information Security" – National Institute of Standards and Technology (NIST);
- "Guideline on Network Security Testing" – NIST;
- "Information Systems Security Assessments Framework" – Open Information Security Group;
- "Durch fuhrungs konzept fur Penetrations-tests" – Bundesamt fur Sicherheit in der Information stechnik (BSI);
- «Open Web Application Security Project» (OWASP).

Аналіз статистичних даних хакерських зломів, а також проведені дослідження показали, що останнім часом все більше кібератак проводиться на веб-ресурси. Загальна методологія проведення pen-тестування веб-ресурсів описана в документах відкритого проекту забезпечення безпеки веб-додатків (OWASP).

Офіційні джерела повідомляють, що учасники спільноти OWASP роблять додатки безпечніше, враховуючи людський фактор і технологічний рівень. При цьому найбільш затребувані документи, опубліковані OWASP, включають в себе: керівництво OWASP [7], оглядове керівництво по коду OWASP [5] і широко застосовуваний проект Топ-10 OWASP [6]. Найпоширенішими інструментами OWASP є тренувальне середовище [4], проксі-аналізатор WebScarab [1] і .NET інструменти [2]. Подібна широта поширення і відкритість документації OWASP з одного боку дозволяє динамічно вдосконалити окремі засоби, методики і механізми проведення тестування, але з іншого ускладнює процес формування загальної методології проведення pen-тестування веб-додатків. Вирішенню цього завдання присвячена ця стаття.

Основна частина

Проведені дослідження показали, що сучасний веб-ресурс є механізмом, що постійно розвивається, оновлюється і удосконалюється. Ці удосконалення націлені на поліпшення продуктивності, підвищення конверсії, оптимізації роботи і зручності використання. Але при цьому з тих чи інших причин можуть бути допущені помилки, які можуть призвести до компрометації веб-ресурсу. Це можуть бути «забу-

ті» службові скрипти, недостатній контроль за даними, відсутність перевірок доступу, висновок різних помилок і багато іншого. Для використовуваної CMS в публічному доступі можуть з'явитися експлоїти, що дозволяють отримати доступ до того чи іншої функціоналу веб-додатків, за допомогою яких зловмисник може завдати шкоди або спробувати отримати критичні дані.

Багато уразливостей, що експлуатуються середньостатистичним зловмисником, лежать на поверхні і не вимагають глибоких знань або кваліфікації для їх експлуатації.

Це в значній мірі розширює масштаби проведення кібератак-«відразу» і збільшує ступінь їх небезпеки.

Для того щоб бути впевненими в тому, що вебдодаток не вдасться зламати кібератакою-«відразу» в статті пропонується кілька сценаріїв перевірки типових векторів атаки на веб-додаток.

Сценарій збору інформації складається з чотирьох етапів, детально представлених на рис. 1. Аналогічно сценарій аналізу інформації та перевірки сайту представлений на рис. 2.

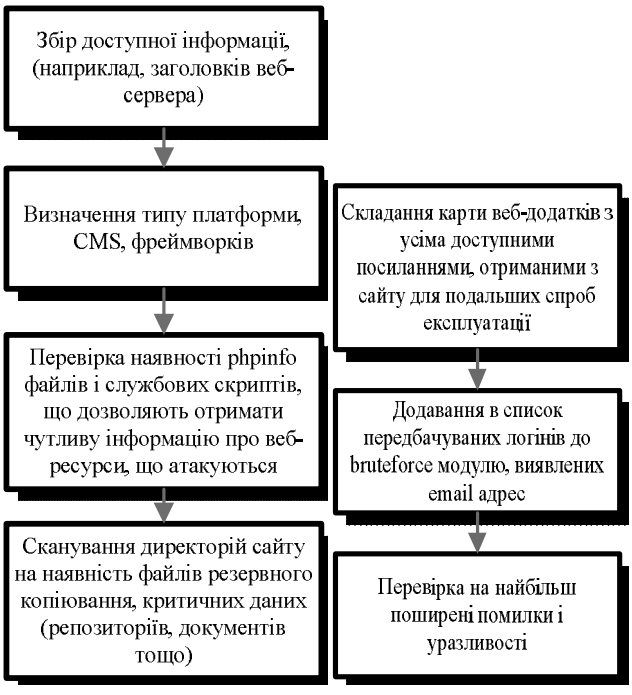

Рис. 1. Сценарії: а – збору інформації; б –аналізу інформації та перевірки сайту

Слід зауважити, що перевірку сайту необхідно здійснювати на найбільш поширені помилки і уразливості, такі як:

- sql injections - різного роду sql ін'єкції;
- cross site scripting - xss, міжсайтовий скриптинг;
- cross site requets forgery - csrf, міжсайтова підробка запитів;
- local file inclusion - локальний інклуд;
- remote file inclusion - віддалений інклуд;
- open redirects - редіректи;
- code executions - виконання коду;
- http response splitting - розщеплення http запитів;
- xpath injections - xpath ін'єкції;
- buffer overflows - різного роду переповнення буфера;
- known vulnerabilities - пошук відомих експлойтів.

Відзначимо, що представлені на рис. 1, 2 сценарії складені з урахуванням методології OWASP TOP 10. Список OWASP Топ-10 заснований на восьми базах даних від семи компаній, включаючи чотири консалтингові фірми і трьох вендорів SaaS. Загальна база містить понад 500 тис. вразливостей в сотнях організацій та тисячах додатків.

- A1 Впровадження коду.
- A2 Некоректна аутентифікація і управління сесією.
- A3 Міжсайтовий скриптинг (XSS).
- A4 Небезпечні прямі посилання на об'єкти.
- A5 Небезпечна конфігурація.
- A6 Витік чутливих даних.
- A7 Відсутність контролю доступу до функціонального рівня.
- A8 Підробка міжсайтових запитів (CSRF).
- A9 Використання компонентів з відомими уразливими.
- A10 Невалідовані редіректи.

Використовуючи дані статистики найбільш поширених кібератак, запропонуємо у вигляді табл. 1 варіант методології тестування веб-додатку.

Наступним кроком в мінімізації ймовірності кібератак на веб-ресурси є ранжування пріоритетності можливих вразливостей системи, аналіз та управління ризиками в процесі розробки і експлуатації ресурсів.

Висновки

У статті представлений варіант методології проведення pen-тестування веб-додатків з прикладом, заснованим на статистичних даних найбільш поширених кібератак.

Частота перевірки (раз в квартал, або частіше, за бажанням) дозволять власнику сайту мати актуальну картину безпеки. Такого роду перевірки дозволять в найкоротші терміни виявити більшість поверхневих вразливостей, застарілі версії ПЗ і компонентів CMS і дозволять оперативно захистити вебдодаток.

Подальші розробки в цьому напрямі повинні вестися в площині класифікації, аналізу та управління окремими рівнями OWASP, розширення і врахування можливих кібератак на веб-ресурси.

Таблиця 1

Варіант методології тестування веб-додатку

Рівень OWASP (тип уразливості)	Можливі прояви	Небезпека
OWASP A1 (injection) – Впровадження коду	Помилки в тілі сторінки, час відгуку.	Компрометація призначених для користувача даних, зараження сайту.
OWASP A2 (broken authentication and session management) – Некоректна аутентифікація і управління сесією	Передача сесії в URL, відсутність шифрування, термін дії сесії, прив'язка до IP-адреси.	Витік чужий сесії може бути призначене перехоплення управління аккаунтом
OWASP A3 XSS (cross-site scripting) – Міжсайтовий скриптинг	Наявність відповіді на спеціально сформований запит в коді сторінки,	Атака проводиться безпосередньо на користувача, маніпуляція даними
OWASP A4 (insecure direct object references) – Небезпечні прямі посилання на об'єкти	Перебір значення параметрів	Можливий витік критичних даних
OWASP A5 (security misconfiguration) – Небезпечна конфігурація	Виявлення налаштувань по замовчуванню, стандартних паролів, повідомлень про помилки	Компрометація призначених для користувача даних, зараження сайту
OWASP A6 (sensitive data exposure) – Витік чутливих даних	Коректна установка і настройка сертифікатів, виявлення критичних даних	Можливий витік критичних даних
OWASP A7 (missing function level access control) – Відсутність контролю доступу до функціонального рівня	Маніпуляція даними для отримання доступу	Можливий витік критичних даних
OWASP A8 CSRF (cross-site request forgery) – Підробка міжсайтових запитів	Відсутність перевірки адреси запиту (токена)	Маніпуляція даними
OWASP A9 (using components with known vulnerabilities) – Використання компонентів з відомими уразливими	Наявність загальнодоступних вразливостей для даної версії програми	Компрометація призначених для користувача даних, зараження сайту
OWASP A10 (unvalidated redirects and forwards) – Невалідовані редіректи	Маніпуляція параметрами URL	Компрометація призначених для користувача даних, можливий витік критичних даних

Список літератури

1. "Ежеквартальная проверка безопасности сайта / [Електронний ресурс]. – Режим доступу до ресурсу: https://habrahabr.ru/company/pentestit/blog/271985/.

2. Семенов С.Г. Исследование методов идентификации програмного обеспечения и их характеристик / С.Г.Семенов // Системи обробки інформації. – Х.: ХУ ПС, 2015. – Вип. 12(137). – С. 148-150.

3. Ткаченко В. Требования к тесту на проникновение [Електронний ресурс] / В. Ткаченко. – Режим доступу: http://auditagency.com.ua/blog/Pentest%20requirements.pdf

4. Cahyo D. Pen test methodology [Електронний ресурс]. – Режим доступу: http://www.slideshare.net/cahyod.

5. Category:OWASP Code Review Project / [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/Category:OWASP_Code_Review_Project.

6. Category:OWASP Top Ten Project / [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/ OWASP_Top_Ten_Project.

7. OWASP Guide Project / [Електронний ресурс]. – Режим доступу: https://www.owasp.org/index.php/OWASP_Guide_Project.

Надійшла до редколегії 12.02.2016

Рецензент: д-р техн. наук, проф. І.В. Рубан, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

МЕТОДОЛОГИЯ ПРОВЕДЕНИЯ PEN-ТЕСТИРОВАНИЯ ВЕБ-ПРИЛОЖЕНИЙ

С.М. Порошин, А.А. Можаев, М.А. Можаев

Проанализированы основные подходы по проведению тестирования на уязвимости информационно-телекоммуникационных и компьютерных систем, сделан выбор направления pen-тестирования веб-ресурсов. Согласно методологии OWASP TOP 10 разработаны сценарии сбора информации, анализа информации и проверки сайта. Определены распространенные ошибки и уязвимости. На основе статистических данных основных опасностей сайта разработан вариант методологии тестирования веб-приложения. Сделан вывод, что дальнейшие разработки в этом направлении должны вестись в плоскости классификации, анализа и управления отдельными уровнями OWASP, расширение и учета возможных кибератак на веб-ресурсы.

Ключевые слова: *pen-тестирования, веб-приложения, сайт, кибер-атаки, хакерские взломы, Open Web Application Security Project.*

METHODOLOGY OF PEN-TESTING WEB APPLICATIONS

S.M. Poroshin, O.O. Mozhaev, M.O. Mozhaev

The basic approaches to testing for vulnerability information and telecommunications and computer systems, the choice of direction made pen-test web resources. According to the methodology OWASP TOP 10 scenarios developed information collection, information analysis and testing site. Determined common mistakes and susceptibility. Based on statistics main dangers website developed methodology variant testing web application. It is concluded that further development in this direction should be conducted in a plane classification, analysis and management of individual levels of OWASP, expansion and consideration of possible cyber attacks on Web resources.

Keywords: *pen-testing, Web application, site, cyber-attacks, hacking hacks, Open Web Application Security Project.*