УДК 004.056 **doi: 10.26906/SUNZ.2019.1.133**

А. Г. Тецький

Національний аерокосмічний університет імені М. Є. Жуковського «ХАІ», Харків, Україна

АНАЛІЗ ПРОБЛЕМ І МОЖЛИВОСТЕЙ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ WEB-ЗАСТОСУНКІВ, СТВОРЕНИХ ЗА ДОПОМОГОЮ СИСТЕМ КЕРУВАННЯ ВМІСТОМ

Дослідження процесів отримання несанкціонованого доступу в системах керування вмістом являє науковий інтерес і дає можливість розробляти ефективні способи захисту від вторгнень. **Предметом** дослідження є процеси оцінювання та забезпечення безпеки Web-застосунків, створених за допомогою систем керування вмістом. **Метою статті** є визначення проблем оцінювання і забезпечення безпеки Web-застосунків. **Результати.** Показано особливості використання систем керування вмістом в якості об'єкта дослідження проблем безпеки. Визначено основні причини успішних атак Web-застосунків. Наведені приклади існуючих методів тестування безпеки, визначено їх переваги та недоліки. Запропоновано комплекс дій, спрямованих на зниження ймовірності успішної атаки. **Висновок.** Визначено проблеми оцінювання та забезпечення безпеки Web-застосунків. Зумовлено необхідність створення методів для вирішення проблем, показано взаємозв'язок вирішуваних завдань.

Ключові слова: атака, безпека, Web-застосунок, система керування вмістом, тестування на проникнення.

Вступ

Системи керування вмістом є програмним забезпеченням, за допомогою якого можна досить швидко і легко створити Web-сайт в мережі Інтернет. Завдяки таким системам, кількість сайтів в мережі безперервно зростає, оскільки для створення сайту не потрібно володіти мовами програмування. Налагодження та управління такою системою відбувається через панель адміністратора за допомогою використання Web-інтерфейсу. Необхідність використання різноманітного функціоналу на сайтах привела до того, що практично всі системи керування вмістом стали мати модульну архітектуру. Використання такого підходу дозволяє додати потрібну функціональність на сайт шляхом установки необхідних доповнень (модулів, плагінів). Однак за великою кількістю переваг систем керування вмістом криються і недоліки, про які власники сайтів часто забувають.

Одним з таких недоліків є проблема безпеки. Практично завжди власник електронного ресурсу не знає про те, які уразливості присутні в коді його сайту. Зростання кількості сайтів в мережі Інтернет супроводжується зростанням інтересу зловмисників в даній сфері [1]. Таким чином, дослідження процесів отримання несанкціонованого доступу в системах керування вмістом являє науковий інтерес і дає можливість розробляти ефективні способи захисту від вторгнень [2].

Метою статті є визначення проблем оцінювання і забезпечення безпеки Web-застосунків, створених за допомогою систем керування вмістом.

Основні результати

Система керування вмістом (англ. CMS – Content Management System) є частиною багатокомпонентної системи, яка забезпечує функціонування Web-застосунка. При оцінюванні безпеки варто пам'ятати про те, що будь-який компонент цієї системи може містити вразливості, які можуть привести до компрометації Web-застосунка. Дослідження уразливостей інших компонентів (наприклад, операційної системи) представляє окрему тему для досліджень.

В даний час для створення Web-застосунків можуть бути використані різні технології і мови програмування. На рис. 1 показаний набір серверного програмного забезпечення LAMP, який найбільш часто застосовується при створенні Web-ресурсів.

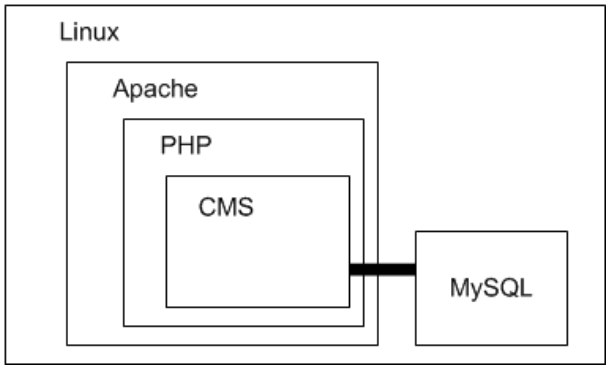

Рис. 1. Набір серверного ПЗ

Системи керування вмістом, створені за допомогою вищевказаних технологій, становлять найбільший інтерес при виявленні проблем безпеки. Згідно зі статистикою, проекти, створені з використанням мови програмування PHP, містять більше уразливостей в порівнянні з проектами, створеними з використанням інших мов програмування. Це зумовлено тим, що мова PHP має низький поріг входження, тобто освоїти цю мову можна з меншими витратами часу.

Можна виділити дві основні причини успішних атак Web-застосунків:

– низький рівень знань в області інформаційної безпеки розробника системи керування вмістом (або її компонента);

– низький рівень знань в області інформаційної безпеки адміністратора системи керування вмістом.

Перша причина виходить з того, що досить тривалий час проблемам безпеки не приділялася

належна увага. Розробник пише код, який виконує необхідну функціональність, і не думає про те, до яких наслідків може привести його помилка у вигляді забутої перевірки будь-якої умови або параметра. З іншого боку, замовник теж не завжди зацікавлений у написанні безпечного коду. Замовник зацікавлений в створенні нових переваг свого сайту серед конкурентів, що повинно приводити до збільшення прибутку. Він може просто не розуміти, до яких наслідків може привести злом його сайту.

Друга проблема стосується суспільства в цілому. Далеко не всі розуміють, чому не можна встановлювати на свій комп'ютер програмне забезпечення з недостовірних джерел, чому не можна вказувати легкі паролі при реєстрації де-небудь і т.д. Від власників сайтів можна почути фразу «Навіщо комусь потрібно зламувати мій сайт?». Відповідаючи на це питання, варто пам'ятати, що атаки бувають таргетовані та нетаргетовані, тобто з певною метою (об'єктом) атаки або ж без неї [3]. Навіть якщо власник ресурсу впевнений в тому, що його сайт не може бути об'єктом цільової атаки, сайт все одно може бути атакований внаслідок нетаргетованої атаки. Боти, що працюють в автоматичному режимі, можуть потрапити на будь-який сайт і провести якусь послідовність атак (наприклад, пошук і експлуатація відомих уразливостей або перевірка наявності обробки вхідних даних). Якщо сайт був успішно атакований або за будь-якими ознаками проявив схильність до успішної атаки, бот повідомляє інформацію про цей сайт зловмисникові, і тоді цей сайт може бути зламаний за участю людини і додаткових інструментів. Під зломом і успішної атакою мається на увазі отримання несанкціонованого доступу до панелі управління сайтом.

Ті власники сайтів, які розуміють, до чого може привести злом їх сайту, починають цікавитися тим, наскільки легко їх сайт зламати. Виникає необхідність оцінювання ймовірності успішної атаки Web-застосунка [4].

Існуючі напрацювання в цій галузі в більшості випадків націлені на проведення тестування безпеки, а не на оцінювання ймовірності успішної атаки в цілому. Наприклад, проектом OWASP був розроблений перелік конкретних завдань під назвою «Web Application Security Testing Cheat Sheet», які повинні бути перевірені тестувальником в процесі пошуку проблем безпеки [5]. Знайдені проблеми можуть перетинатися з критичними проблемами безпеки, описаними цим же проектом в документі «OWASP Top 10 – 2017 The Ten Most Critical Web Application Security Risks» [6]. У цьому документі показані 10 найбільш критичних проблем безпеки Web-застосунків. Кожна проблема має якісні показники, такі як можливість злому, поширеність, можливість виявлення і критичність наслідків. Базуючись на цих показниках, можна отримати якісну оцінку за показником «Можливість зламу», розглядаючи тільки проблеми з високою критичністю наслідків.

Описаний вище метод націлений на виявлення проблем безпеки, які могли бути допущені розробниками при створенні Web-застосунка. Але не варто забувати про другу причину успішних атак – про адміністраторів систем керування вмістом. Загальні правила щодо складності паролів, зберігання паролів, передачі прав доступу і т.п. повинні регламентуватися за допомогою політики безпеки. Процес перевірки наявності політик безпеки і їх дотримання називається Web-аудитом. У результаті його проведення можна отримати лише відсоток покриття вимог, однак само по собі це число ні про що не говорить, оскільки порушення різних вимог мають різну критичність.

Підводячи підсумок вищесказаного, слід акцентувати увагу на тому, що результати тестування на проникнення і результати Web-аудиту окремо не можуть дати кількісну оцінку ймовірності успішної атаки. Тому необхідний метод оцінювання, заснований на результатах тестування на проникнення і Web-аудиту.

Після оцінювання ймовірності успішної атаки може виникнути необхідність у зниженні розрахованої ймовірності. Це може бути досягнуто за допомогою впровадження додаткових заходів захисту Web-застосунка, проведення тренінгів для персоналу, що використовує системи керування вмістом, і т.п. Розглянемо деякі дії по захисту Web-застосунка докладніше.

Проведення тренінгів для персоналу необхідно для підвищення загального рівня знань в області інформаційної безпеки. Співробітники повинні розуміти, до чого може привести використання легких паролів, зберігання паролів в різному вигляді, використання програмного забезпечення невідомого походження.

Налаштування захищеного з'єднання дозволяє запобігти перехоплення чутливих даних при передачі. Дослідження компанії SEMrush на вибірці з 100000 сайтів показали, що захищене з'єднання використовують близько 31,5% сайтів [7]. Цей показник був актуальний в 2017 році, в 2014 році цей же показник був близько 7,6%. В даний час багато хостинг-провайдерів полегшують процес отримання сертифікату для шифрування даних. Раніше компанія Google повідомила, що використання шифрування матиме позитивний вплив на ранжування [8].

Установка та налаштування файрволу ускладнює або унеможливлює експлуатацію уразливостей і проведення деяких інших атак. Наприклад, використання брандмауера ModSecurity є безкоштовним, але його необхідно налаштувати для максимально ефективного використання, щоб запобігти якомога більше атак і при цьому не нашкодити працездатності самої системи керування вмістом.

Усі ці заходи вимагають фінансових затрат і заздалегідь невідомо, наскільки ці заходи будуть ефективні. Коефіцієнти впливу можуть бути визначені тільки шляхом експертних оцінок. Потрібен метод вибору найбільш ефективних контрзаходів в умовах обмеженого бюджету [9, 10].

Моделювання впливу контрзаходів на показник успішності атаки дозволяє побудувати графік залежності показника успішності атаки від загальної вартості послуг із захисту Web-застосунка. Викори-

стовуючи такий графік, можна приймати рішення з приводу доцільності використання тих чи інших заходів захисту. Приклад такого графіка показаний на рис. 2. У статті [11] описаний метод вибору заходів захисту, який дозволяє отримати графічне представлення залежності показника успішності атаки від бюджету. Послуги по створенню сайтів і вирішенню проблем безпеки найчастіше надаються організаціями або фізичними особами. Але також бувають випадки, коли майбутній власник сам займається налаштуванням і створенням сайту. У разі небажання або неможливості звернення до організацій, що надають послуги в сфері інформаційної безпеки Web-застосунків, власник може сам провести оцінювання ймовірності успішної атаки свого сайту. В цьому випадку визначити достовірність оцінки неможливо. Оскільки в процесі оцінювання необхідно проведення тестування на проникнення, яке майже завжди проводиться з використанням інструментальних засобів, то необхідно створити агрегатор, який буде містити інформацію про інструментальні засоби. Такий сервіс повинен допомогти вибрати інструментальний засіб для вирішення конкретного завдання тестування на проникнення.

Взаємозв'язок завдань оцінювання і зниження ймовірності успішної атаки, а також завдання вибору інструментальних засобів тестування на проникнення, показано на рис. 3.

Передбачаються такі варіанти розвитку подій:

1. Власник електронного ресурсу звертається до особи / організації, яка проводить оцінювання (постачальник послуг). Власник виявився задоволений результатами оцінювання і не має бажання замовляти послуги щодо зниження ймовірності успішної атаки. Такий сценарій можна позначити літерою «О».

2. Після оцінювання у власника є бажання знизити ймовірність успішної атаки. Постачальник послуг вказує вартість послуг і відповідні коефіцієнти впливу кожної послуги. Будується графік залежності ймовірності успішної атаки від загальної вартості послуг. Власник визначає допустимий бюджет, постачальник послуг надає вибрані послуги. Такий сценарій позначається буквами «О – З».

3. Власник має можливість і бажання самостійно провести оцінювання, але він не є компетентним фахівцем в питаннях інформаційної безпеки і не знає, які інструментальні засоби необхідно використовувати. Власник електронного ресурсу вибирає необхідні інструменти і проводить оцінювання самостійно. Такі сценарії будуть позначені «В – О» і «В – О – З» відповідно, в залежності від необхідності проведення зниження ймовірності успішної атаки.

Пунктирна стрілка «З – О» показує можливе бажання власника електронного ресурсу заново провести оцінювання після проведення заходів щодо зниження ймовірності успішної атаки.

Виходячи з усього вищесказаного, виникає необхідність створення методів оцінювання та забезпечення безпеки систем керування вмістом, а також методу вибору інструментальних засобів тестування на проникнення.

Створені рішення будуть корисні постачальникам послуг в сфері інформаційної безпеки Web-застосунків, а також особам, які бажають підвищити рівень знань в цій же сфері.

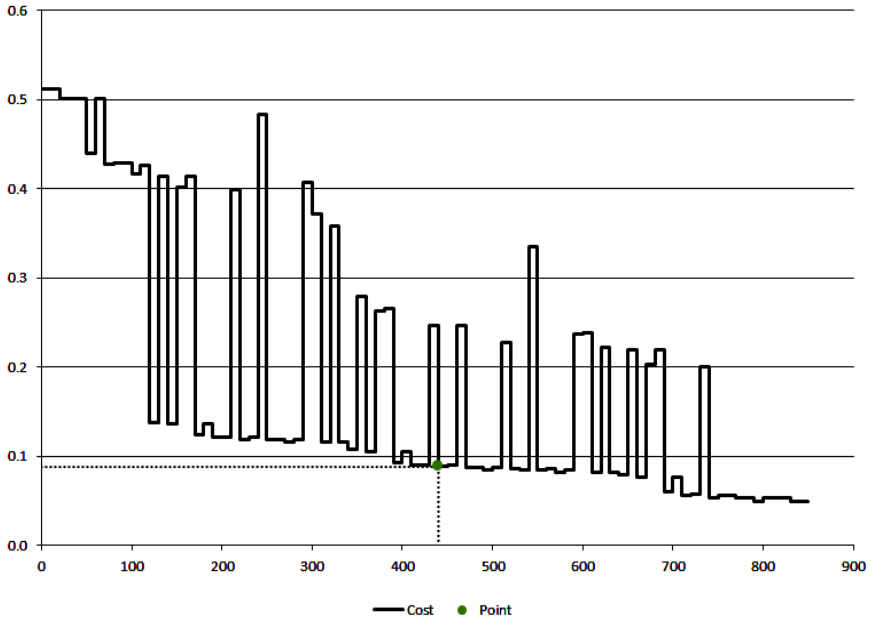

Рис. 2. Графік залежності показника успішності атаки від бюджету

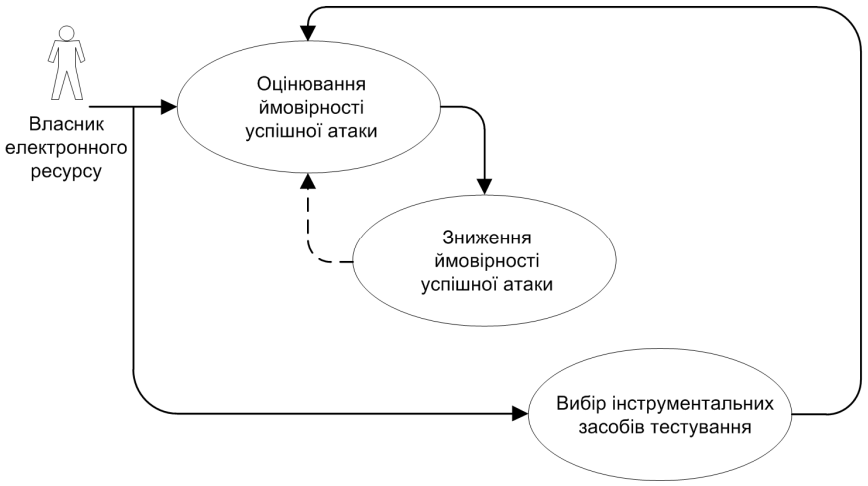

Рис. 3. Взаємозв'язок завдань

Висновок

У даній статті були визначені основні причини успішних атак Web-застосунків, показані особливості дослідження проблем безпеки систем керування вмістом. Наведені приклади існуючих методів тестування безпеки, визначені їх переваги та недоліки. Запропоновано комплекс дій, спрямований на зниження ймовірності успішної атаки. Також визначені проблеми оцінювання та забезпечення безпеки Web-застосунків.

Зумовлено необхідність створення методів для вирішення проблем, показано взаємозв'язок вирішуваних завдань.

СПИСОК ЛІТЕРАТУРИ

1. Hacked Website Report 2017 [Електронний ресурс] – Режим доступу: https://sucuri.net/reports/Sucuri-Hacked-Report-2017.pdf (дата звернення: 10.12.2018)
2. WAF and IPS. Does your environment need both? [Електронний ресурс] – Режим доступу: https://cybersins.com/security-waf-ids-dilemma/ (дата звернення: 09.12.2018)
3. Sood, A. K. Targeted cyberattacks: a superset of advanced persistent threats / A. K. Sood, R. J. Enbody // IEEE security & privacy. – 2013. – Vol. 11(1). – P. 54-61.
4. А. Г. Тецкий. Применение деревьев атак для оценивания вероятности успешной атаки web-приложения // Радіоелектронні і комп'ютерні системи. – 2018. – № 3. – С. 74–79.
5. Web Application Security Testing Cheat Sheet [Електронний ресурс] – Режим доступу: https://www.owasp.org/index.php/Web_Application_Security_Testing_Cheat_Sheet (дата звернення: 05.12.2018)
6. OWASP Top 10 – 2017 The Ten Most Critical Web Application Security Risks [Електронний ресурс] – Режим доступу: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (дата звернення: 10.12.2018)
7. Why You Should Move Your Site to HTTPS: SEMrush Data Study [Електронний ресурс] – Режим доступу: https://www.semrush.com/blog/why-you-should-move-your-site-to-https-semrush-data-study/ (дата звернення: 01.12.2018)
8. HTTPS as a ranking signal [Електронний ресурс] – Режим доступу: https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html (дата звернення: 05.12.2018)
9. Kuchuk G.A. An Approach To Development Of Complex Metric For Multiservice Network Security Assessment / G.A. Kuchuk, A.A. Kovalenko, A.A. Mozhaev // Statistical Methods Of Signal and Data Processing (SMSDP – 2010): Proc. Int. Conf., October 13-14, 2010.– Kiev: NAU, RED, IEEE Ukraine section joint SP, 2010. – P. 158 – 160.
10. Saravana Balaji B., Amin Salih Mohammed, Chiai Al-Atroshi, "Adaptability of SOA in IoT Services – An Empirical Survey", Int. Journal of Computer Applications, vol. 182(31), pp. 25-28, 2018, DOI: http://doi.org/10.5120/ijca2018918249
11. Tetskyi A. The method of selecting measures to protect the Web application against attacks // Сучасні інформаційні системи. – 2018. – Т. 2, № 4. – С. 114–118.

Рецензент: д-р техн. наук, проф. Г. А. Кучук,
Національний технічний університет «ХПІ», Харків
Received (Надійшла) 13.10.2018
Accepted for publication (Прийнята до друку) 26.12.2018

Анализ проблем и возможностей обеспечения безопасности Web-приложений, созданных с помощью систем управления контентом

А. Г. Тецкий

Исследование процессов получения несанкционированного доступа в системах управления содержимым представляет научный интерес и дает возможность разрабатывать эффективные способы защиты от вторжений. **Предметом** исследования являются процессы оценивания и обеспечения безопасности Web-приложений, созданных с помощью систем управления контентом. **Целью** статьи является определение проблем оценивания и обеспечения безопасности Web-приложений. **Результаты.** Показаны особенности использования систем управления контентом в качестве объекта исследования проблем безопасности. Определены основные причины успешных атак Web-приложений. Приведены примеры существующих методов тестирования безопасности, определены их достоинства и недостатки. Предложен комплекс действий, направленный на снижение вероятности успешной атаки. **Заключение.** Определены проблемы оценивания и обеспечения безопасности Web-приложений. Обусловлена необходимость создания методов для решения проблем, показана взаимосвязь решаемых задач.

Ключевые слова: атака, безопасность, Web-приложение, система управления контентом, тестирование на проникновение.

Analysis of problems and opportunities for ensuring the security of Web applications created with using content management systems

A. Tetskyi

Investigation of the processes of obtaining unauthorized access in content management systems is a scientific interest and provides an opportunity to develop effective methods of protection from intruders. The **subject matter** of the research is the processes of evaluating and ensuring the security of Web applications created with using content management systems. The **goal** of the paper is to determine the problems of evaluating and ensuring the security of Web applications. **Results**. The features of the use of content management systems as an object of research security issues are shown. The main reasons of successful attacks of Web applications are identified. Examples of existing security testing methods are shown; their advantages and disadvantages are identified. A set of actions aimed at reducing the successful attack probability is proposed. **Conclusion**. The problems of evaluating and ensuring the security of Web applications are identified. The need of creation methods to solve problems is determined; the relationship of tasks is shown.

Keywords: attack, security, Web application, content management system, penetration testing.