УДК 004.738.52

Д. П. Присяжний
Вінницький національний технічний університет
Хмельницьке шосе, 95, 21021 Вінниця, Україна

Удосконалення захисту веб-ресурсів від атак на основі комбінованого евристично-статистичного підходу

Описано удосконалення захисту веб-ресурсів від атак, що базується на використанні комбінованого евристично-статистичного підходу. Захист використовує класифікацію найбільш розповсюджених атак, ймовірність даної атаки та евристичні заходи вибору протидії атаці.

***Ключові слова**: веб-ресурс, атака, захист, статистичні дані, евристичні методи.*

Вступ

Захист веб-ресурсів залишається одним із важливих напрямків інформаційної безпеки. Щороку кількість веб-ресурсів збільшується, зростає також кількість конфіденційної інформації, яка локалізується на серверах віддаленого доступу (особливо із використанням хмарних технологій).

У результаті цього зростають не тільки кількість атак на веб-ресурси, але й економічні наслідки таких атак. Останнім часом вразливість веб-ресурсів до атак отримала політичний вимір унаслідок як поширення гібридних війн у світі, так і зростання терористичних загроз.

Таким чином, удосконалення методів і систем захисту веб-ресурсів від атак залишається актуально науковою проблемою, особливо з урахуванням постійного вдосконалення методів та інструментів атак і появи нових методів та інструментів. Удосконалення методів захисту веб-ресурсів від атак є також важливою в практичному застосуванні задачею внаслідок зростаючих економічних, соціальних і політичних наслідків від зловмисних дій.

Аналіз публікацій та постановка задачі

Проблемам захисту веб-ресурсів присвячене широке коло досліджень. Наприклад, книги [1, 2], які повністю присвячені опису методів та інструментів атак і захисту від них. Видані з інтервалом майже в 10 років, вони наочно ілюструють зміни в підходах до захисту веб-ресурсів. Якщо в [1] стверджується про можливість

забезпечення захисту від будь-яких атак на веб-ресурси, то в [2] розглянуто конкретні методи для захисту від атак. Така зміна орієнтування викладу є дуже симптоматичною та є наслідком тієї обставини, що методи та інструменти атак досить важко піддаються класифікації, а сама атака часто використовує технології маскування цих методів та інструментів.

У [3] описано метод ідентифікації атак типу «відмова в обслуговуванні», оснований на застосуванні багатошарового персептрону, що дозволило отримати необхідну множину показників.

Розв'язання задачі детектування DDoS-атак на основі розробки спеціальної метрики є предметом статті [4]. В роботі [5] проаналізовано існуючі методи захисту від DDoS-атак і запропоновано новий метод, який базується на статистичному аналізі вхідного трафіка на сервері та надійній системі перевірки гіпотез.

Розробляють також комбіновані методи захисту веб-ресурсів, основані на використанні евристичного підходу [6], в рамках якого виділяється аномальна поведінка споживача, що підвищує ймовірність захисту порівняно із сигнатурним аналізом.

Перспективним також є використання моделей агента загроз для захисту веб-ресурсів від атак [7], що дозволяє формалізувати пошук вразливостей в інформаційних системах на всіх етапах взаємодії агента загроз із веб-ресурсом.

Розгляд Cross-site scripting атак на Android WebView здійснено в [8], де розроблено метод моніторингу доступу для браузера з метою протидії.

Проблеми витоку інформації проаналізовано в [9, 10], де розглянуто як типові сценарії, так і методи та способи захисту від них.

У [11] відмічено, що злам паролю залежить від наявних обчислювальних ресурсів, часу, функції, що використовується для зберігання цього пароля, а також від багатьох інших характеристик. Запропоновано загальні рамки для оцінки складності пароля й оцінки його надійності.

Метою статті є удосконалення захисту веб-ресурсів від атак, яке базується на використанні комбінованого евристично-статистичного підходу.

Аналіз актуальних атак на веб-ресурси

Аналіз здійснено із використанням існуючих статистичних даних за 2015 рік [12]. Наведено не тільки опис атак і відсоток веб-ресурсів, до яких вони можуть бути застосовані, але також і запропоновані автором адекватні методи протидії таким атакам. Для наочності результати зведено в таблицю.

Найбільш популярною атакою є «Insufficient transport layer protection» — отримання даних під час передавання. Дана атака може бути виконана для 70 % ресурсів. Для виключення можливості проведення таких атак достатньо використовувати протокол HTTPS.

Витік інформації («Information leakage»). Дану атаку можна виконати на 56 % ресурсів. Витік інформації з додатків виникає в результаті відмови або неправильної роботи програми, а також у разі порушення її логіки. Для виключення можливості проведення атаки необхідно ретельно тестувати програмну частину ресурсу, проводити перевірку повідомлень на стороні сервера, моніторинг оповіщень про помилки.

Класифікація видів атак, їхня розповсюдженість і методи протидії

№ за/п	Вид атаки	Вразливість веб-ресурсів, %	Протидія
1	Insufficient transport layer protection	70 %	Використання протоколу HTTPS.
2	Information leakage	56 %	Тестування програмної частини ресурсу, перевірка повідомлень на стороні сервера, моніторинг оповіщень про помилки
3	Cross-site scripting	47 %	Очищення та валідація вхідних даних
4	Brute force	29 %	Використання паролів високої складності, налаштування сервера на аналіз вхідних запитів
5	Content spoofing	26 %	Відмовитися від використання фреймів і не передавати в параметрах абсолютні або локальні шляхи до файлів
6	Cross-site request forgery	24 %	Перевірка вхідних даних з форм
7	URL redirector abuse	16 %	Валідація вхідних даних
8	Predictable resource location	15 %	Контроль доступу до файлів сервера

Атаку «Cross-site scripting» — міжсайтове використання сценаріїв, можливо виконати на 47 % ресурсів. Атака дозволяє передати JavaScript-код на виконання в браузер користувача. Атаки такого роду часто також називають HTML-ін'єкціями, адже механізм їхнього впровадження дуже схожий із SQL-ін'єкціями, але на відміну від останніх, впроваджуваний код виконується в браузері користувача. Для захисту від цього виду атак необхідно проводити очищення та валідацію вхідних даних.

Генерацію великої кількості запитів, або підбір паролів («Brute force») можливо виконати на 29 % ресурсів. Для захисту необхідно забезпечити використання паролів високої складності, налаштування сервера на аналіз вхідних запитів.

Атака «Content spoofing» — підмінна даних через заміну контенту сторінок можлива для 26 % ресурсів. Використовуючи цю техніку, зловмисник змушує користувача повірити, що сторінка згенерована веб-сервером, а не передана із зовнішнього джерела. Для захисту від даного виду атак потрібно відмовитися від використання фреймів і, найголовніше, ніколи не передавати в параметрах абсолютні або локальні шляхи до файлів.

Вид атак на відвідувачів веб-сайтів, який використовує недоліки протоколу HTTP — «Cross-site request forgery». Якщо жертва заходить на сайт, створений зловмисником, від її особи таємно відправляється запит на інший сервер (наприклад, на сервер платіжної системи), який здійснює якусь шкідливу операцію (наприклад, переказ грошей на рахунок зловмисника). Дану атаку можливо виконати на 24 % ресурсів. Для захисту необхідно проводити перевірку вхідних даних з форм, наприклад шляхом додавання унікального доданка.

Перенаправлення на інші сайти через підміну початкових посилань («URL redirector abuse»). Цей вид вразливостей, також як і багато інших перерахованих вище, є різновидом помилок перевірки вхідних даних і можлива на 16 % ресурсів. Вирішенням є валідація вхідних даних.

Ще однією популярною атакою є «Predictable resource location» — знаходження прихованого функціоналу та даних. Доступна на 15 % ресурсів і вирішується шляхом контролю доступу до файлів сервера.

З кожним роком статистика атак змінюється, так у 2014 році найпопулярнішою була «Cross-site scripting», а в 2013 — Витік інформації («Information leakage»). Виходячи з наведених даних, можна зробити висновки про те, що для захисту від більшості популярних видів атак достатньо належним чином перевіряти вхідні дані. Також рекомендовано використовувати шифрований протокол HTTPS та будувати програмний додаток ресурсу на одному з відомих програмних каркасів (Frame-work), в якому вбудовані механізми перевірки, шифрування та валідації. Також варто зауважити що в даній статті не розглянуті атаки на мережеві служби, наприклад DoS та DDoS. Найкращим методом захисту від яких є використання хмарних технологій і перевірених конфігурацій серверів.

Удосконалений метод захисту веб-ресурсу

Як свідчать статистичні результати [12] та запропоновані методи, які орієнтовані на захист від конкретного типу атаки, зловмисна дія на веб-ресурс відбувається, як правило, із використанням відразу декількох різних типів атак. Тому задачею системи менеджменту інформаційної безпеки є розробка ефективної стратегії протидії атакам зловмисників за умови, що вони використовують комбіновані типи атак. Рівень ефективності при цьому визначається замовником веб-ресурсу і задається він специфікою ведення бізнесу підприємством (чи діяльністю організації), параметрами, що характеризують специфіку інформації та баз даних, які належать до конфіденційних і рядом інших параметрів і характеристик.

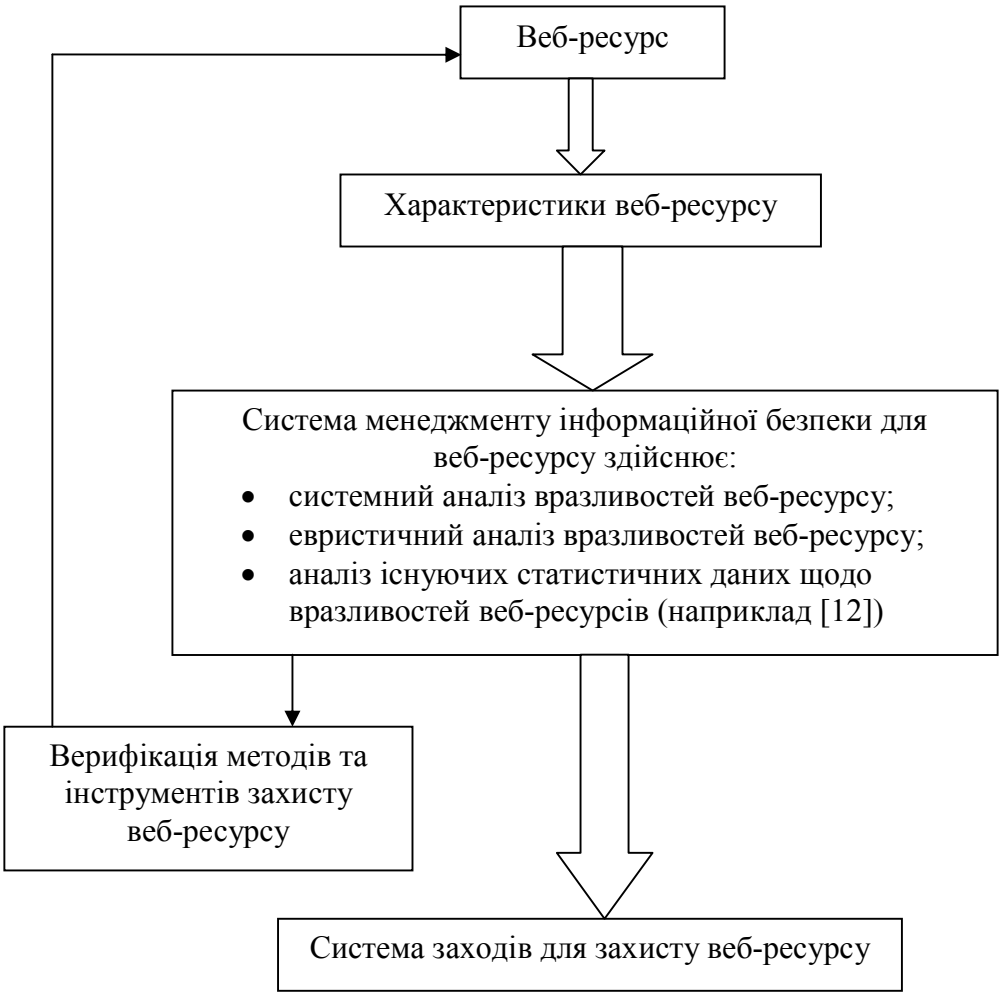
Розробка такої стратегії захисту веб-ресурсу є нетривіальною задачею. Наведемо удосконалений метод захисту веб-ресурсу, який відрізняється від аналогів одночасним здійсненням системного, евристичного та статистичного аналізу вразливостей веб-ресурсу, що дозволяє здійснити якісний захист від зловмисників, які використовують декілька типів атак.

Метод захисту веб-ресурсу можна подати у такій формі (структура методу схематично подана на рисунку).

Етап 1. Формується множина M характеристик веб-ресурсу. Вона включає в себе бази даних/знань, які потрібно захистити від атак, а також характеристики, які описують існуючі системи захисту (наприклад, які інтегровані в хмарні сховища, у використане ліцензійне програмне забезпечення тощо). Також до цієї множини відносяться характеристики, які визначають специфічні методи та технології взаємодії із користувачами веб-ресурсу (власне, саме для задоволення потреб користувачів його і створено).

Етап 2. Множина M характеристик веб-ресурсу передається до Системи менеджменту інформаційної безпеки для веб-ресурсу, який здійснює аналіз існуючих вразливостей і розробляє систему заходів для захисту веб-ресурсу. Ця діяль-

ність, що описана в етапах 3–5, здійснюється в паралельному режимі за достатніх ресурсів чи у послідовному режимі, коли наявних ресурсів замало



Структура методу формування системи захисту веб-ресурсу

Етап 3. Здійснюється системний аналіз вразливостей веб-ресурсу до атак. Задачею цього аналізу є: знаходження множини T цілей для атак і множини цілей TP для захисту веб-ресурсу; аналіз обмежень як технічного, так і програмного та інформаційного характеру; аналіз простору альтернатив A (як для здійснення атак на веб-ресурс, так і для його захисту); вибір критеріїв ефективності C захисту веб-ресурсу; синтез адекватної моделі для системи захисту веб-ресурсу; розробка рекомендацій R для впровадження.

Етап 4. Здійснюється евристичний аналіз вразливостей веб-ресурсу. Для цього можуть бути використані, наприклад, нейронні класифікатори [6], онтології [13] чи експерті методи [14] тощо. Цей етап є необхідним, так як робота веб-ресурсу із користувачами є слабоформалізованою, і тому для неї часто неможливо знайти адекватні моделі та методи формального опису. До того ж на цьому етапі також здійснюється аналіз поведінки можливих зловмисників і прогнозування ти-

пів атак, які вони можуть використати. Підкреслимо, що з року в рік статистичний розподіл відсотка застосовуваних зловмисниками атак змінюється, — але поки що неможливе здійснення статистично достовірного прогнозування такої зміни [12].

Етап 5. Здійснюється аналіз для статистичних даних щодо поточного стану вразливостей конкретного веб-ресурсу із використанням існуючих статистичних баз даних, які носять загальний характер [12]. Як правило, виділяється пул найбільш уживаних типів атак на веб-ресурс і використовуються такі методи протидії, які можна застосувати для декількох типів атак. Наприклад, як видно із таблиці, для атак «Cross-site request forgery» та «URL redirector abuse» методи протидії локалізуються на вхідних даних.

Етап 6. За результатами здійсненого аналізу у пп. 3–5 Система менеджменту інформаційної безпеки для веб-ресурсу формує систему заходів (узгоджених між собою методів та інструментів) для захисту заданого веб-ресурсу.

Етап 7. Здійснюється верифікація запропонованої системи захисту веб-ресурсу від атак. Для цього можуть бути використані існуючі та розроблені тестові комп'ютерні програми, задіяні спеціалісти з перевірки захищеності від атак тощо. У разі виявлення недостатнього рівня захисту веб-ресурсу, що виражається у невідповідності характеристик захисту множині критеріїв C, розробленої на етапі 2, етапи 1–6 повторюються.

Етап 8. У випадку, коли досягнуто заданого рівня захисту, система захисту даного веб-ресурсу фіксується та впроваджується.

У разу потреби, запропонований метод повторюється із потрібною періодичністю.

Висновки

Описано удосконалення захисту веб-ресурсів від атак, який на відміну від існуючих, базується на одночасному здійсненні системного, евристичного та статистичного аналізів вразливостей ресурсу, що дозволяє здійснити якісний захист веб-ресурсу від атак. Запропонована система захисту веб-ресурсу використовує віднесення ресурсу до вразливості стосовно певного виду атак.

1. *Скембрейц Дж.* Безопасность Web-приложений — готовые решения / Дж. Скембрейц, М. Шема. — М.: Издательский дом «Вильямс», 2003. — 384 с.

2. *Жуков Ю.В.* Основы веб-хакинга: нападение и защита / Ю.В. Жуков. — СПб.: Питер, 2011. — 176 с.

3. *Сорокин С.Н.* Метод обнаружения атак типа «отказ в обслуживании» на WEB-приложения / С.Н. Сорокин // Прикладная дискретная математика. — 2014. — № 1(23). — С. 55–64.

4. *Фаткиева Р.Р.* Разработка метрик для обнаружения атак на основе анализа сетевого трафика / Р.Р. Фаткиева // Вестник Бурятского государственного университета. — 2013. — Vol. 9.— С. 81–86.

5. *Sen J.* A Robust Mechanism for Defending Distributed Denial OF Service Attacks on Web Servers / J. Sen // International Journal of Network Security & Its Applications (IJNSA). — 2011, March. — Vol. 3, N 2. — P. 162–179.

6. *Поворознюк А.И.* Совершенствование защиты Web-приложений от вторжений на основе эвристического похода / А.И. Поворознюк, М.Н. Шкарупа: сб. науч. тр. «Вестник НТУ «ХПИ». Інформатика і моделювання. — 2007. — Вип. 19. — С. 145–154.

7. *Аласенко А.В.* Разработка и системный анализ математической модели угроз, модели нарушителя, процедур защиты WEB-приложений на всех этапах функционирования / А.В. Аласенко, П.И. Дзьобан // Научный журнал КубГАУ. — 2014. — № 101(07). — С. 1–11.

8. *Bhavani A.B.* Cross-site Scripting Attacks on Android WebView / A.B. Bhavani // International Journal of Computer Science and Network. — 2013. — Vol. 2, Issue 2. — 5 p. ─ Режим доступу в Інтернет: http://ijcsn.org/IJCSN-2013/2-2/IJCSN-2013-2-2-03.pdf

9. *Cuff P.* Distributed channel synthesis / P. Cuff // IEEE. Trans. Inf. Theory. — 2013. — Vol. 59(11). — P. 7071–7096.

10. Schieler C. Rate-distortion theory forsecrecy systems / C. Schieler, P. Cuff // IEEE Trans. on Inf. Theory. — 2014. — Vol. 66(12). — P.7584–7605.

11. *Sahin C.S.* General Framework for Evaluating Password Complexity and Strength / C.S. Sahin, R. Lychev, N. Wagner. — 11 p. — Режим доступу в Інтернет: http://arxiv.org/abs/1512.05814

12. *Website* Security Statistics Report: 2015. — WhiteHat Security, 2015. — 30 p. ─ Режим доступу в Інтернет: https://info.whitehatsec.com/Website-Stats-Report-2015.html

13. *Handbook* on Ontologies / eds. S. Staab and R. Studer. — International Handbooks on Information Systems. — Berlin: Springer, 2009. — 832 p.

14. *Новиков Д.А.* Теория управления организационными системами / Д.А. Новиков. — М.: Физматлит, 2007. — 584 с.

Надійшла до редакції 15.03.2016