СИСТЕМИ УПРАВЛІННЯ

УДК 004.056

Барибін О.І.

МЕТОДОЛОГІЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ ВЕБ-САЙТУ ЗАКЛАДУ ВИЩОЇ ОСВІТИ

У статті розглянуто проблему контролювання якості кіберзахисту веб-сайту закладу вищої освіти, використовуючи технології тестування на проникнення. На основі аналізування сучасних методологій тестування на проникнення запропоновано методологію, яка складається з трьох етапів (перший – збирання інформації та її аналізування; другий – тестування керування конфігурацією та тестування керування сесіями; третій – звітування й переведення системи в початковий стан). Результати досліджень щодо типових вразливостей для веб-сайтів університетів України дали змогу обмежити можливу поверхню атаки, що пришвидшить пошук та аналізування вразливостей на першому етапі запропонованої методології.

***Ключові слова**: тестування на проникнення, веб-сайт, OWASP, OWASP ZAP*.

Постановка проблеми в загальному вигляді та формулювання мети

У сучасному світі більшість сервісів та інформації, з якою контактує споживач, сконцентровано на веб-сайті установи. В умовах конкурентної боротьби між закладами вищої освіти питання якості веб-сайту з точки зору забезпечення його кіберзахисту набуває все більшого значення. Однією з відомих форм для оцінювання стану кібербезпеки та зменшення ризиків кібербезпеки є тестування на проникнення (penetration testing або pentest). Тестування на проникнення – це контрольований експеримент з метою проникнення в систему або мережу для виявлення вразливостей [1]. Тестування на проникнення застосовує ті самі методи, які використовують у разі звичайного нападу зловмисника. Такий підхід дає можливість використовувати відповідні заходи для усунення вразливостей, перш ніж їх вивчать неавторизовані особи.

У праці [2] зазначено такі чотири основні проблемні напрями досліджень, пов’язані з тестуванням на проникнення:

1) основні інструменти, що їх використовують для тестування на проникнення;
2) сценарії атак;
3) методології й стандарти тестування на проникнення;
4) проблемні питання й напрями досліджень.

Треба зазначити, що інструментарію та сценаріям атак у літературі приділено досить багато уваги. Зокрема, можна згадати такі публікації, як [1, 3, 4], у яких досить докладно викладено два питання, зазначені вище. Проте саме наявність в установі чітко окресленої методології тестування на проникнення є запорукою системного визначення й перегляду рівня кіберзахисту.

Отже, визначення вразливостей та складників кіберзахисту веб-сайтів закладів вищої освіти та їх систематизація є **актуальною** проблемою.

Відповідно **мета** роботи – формулювання методології на проникнення, яка враховуватиме специфіку кіберзахисту веб-сайту закладів вищої освіти.

У рамках цієї мети можна визначити такі основні **завдання** праці:

- на основі аналізування сучасних методологій тестування на проникнення визначити етапи, достатні для тестування на проникнення веб-сайту закладу вищої освіти;
- з'ясувати типи вразливостей, характерні для веб-сайтів університетів України;
- запропонувати реалізацію процесу тестування на проникнення.

Аналіз останніх досліджень і публікацій.

Загалом методологія – це схема, яку використовують для досягнення мети. Відмова від використання методології для тестування на проникнення може призвести до неповного випробування, високих витрат часу, невдач та неефективності тестування [5].

Ґрунтуючись на працях [5–11], можна сформувати актуальний перелік сучасних і чинних методологій тестування на проникнення, які загалом можна використовувати для веб-застосувань:

1) Open Source Security Testing Methodology Manual (OSSTMM). Джерело для ознайомлення: http://www.isecom.org/research/osstmm.html;

2) OWASP testing guide. Джерело для ознайомлення: https://www.owasp.org/index.php/OWASP_Testing_Project;

3) Information Systems Security Assessment Framework (ISSAF) Джерело для ознайомлення: www.oissg.org/issaf.html;

4) Penetration Testing Execution Standard (PTES) Джерело для ознайомлення: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines;

5) NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment (NIST SP 800-115). Джерело для ознайомлення: http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

Серед перелічених вище на докладніший розгляд заслуговує методологія OWASP (Open Web Application Security Project). Це пояснюється тим, що ця неприбуткова всесвітня організація об'єднує фахівців у різних галузях для розроблення стандартів безпеки, методик тестування та інструментів саме за напрямом веб-технологій. Так, у праці [9] наведено результати спроби сформулювати просту методологію тестування на проникнення, яка ґрунтується на OWASP Top Ten. Це список із десяти найнебезпечніших та використовуваних векторів атак на веб-застосування, який наразі складається з таких категорій вразливостей [12]:

- A1:2017 Injection,
- A2:2017 Broken Authentication,
- A3:2017 Sensitive Data Exposure,
- A4:2017 XML External Entities (XXE),
- A5:2017 Broken Access Control,
- A6:2017 Security Misconfiguration,
- A7:2017 Cross Site Scripting (XSS),
- A8:2017 Insecure Deserialization,
- A9:2017 Using Components with Known Vulnerabilities,
- A10:2017 Insufficient Logging &Monitoring.

Проте результати роботи мають наразі невеликий рівень актуальності й застосовності з двох причин: список OWASP Top Ten відтоді актуалізовано, а загальний характер запропонованої методології фактично унеможливлює оптимізацію зусиль тестувальника, оскільки фактично не зменшує можливої поверхні атаки (загальна кількість можливих вразливих місць у системі).

Загальні положення методології

Згідно з [6] загалом методологія тестування на проникнення має складатися з трьох

блоків:

- збирання інформації та її аналізування;
- підготування до тестування та проведення тестування;
- звітування та переведення системи в початковий стан.

Як зазначено вище, за основу візьмемо методологію OWASP, яка в оригіналі складається з таких етапів [13]:

1) збирання інформації (Information Gathering);
2) тестування керування конфігурацією (Configuration Management Testing);
3) тестування автентифікації (Authentication Testing);
4) тестування керування сесіями (Session Management Testing);
5) тестування авторизації (Authorization Testing).

Для веб-сайту закладу вищої освіти етапи 3 та 5 мають низьку значимість, оскільки більшість користувачів не повинні бути обов'язково зареєстрованими. З огляду на це можна сформулювати синтетичну методологію, поєднавши структуру в загальному вигляді та модифіковану OWASP методологію:

1) збирання інформації та її аналізування;
2) тестування керування конфігурацією та тестування керування сесіями;
3) звітування й переведення системи в початковий стан.

Специфікація поверхні атаки

Щоб зменшити можливу поверхню атаки на етапі збирання інформації, проаналізуємо найпоширеніші типи вразливостей для веб-сайтів закладів вищої освіти. Для цього використаємо застосування, яке також розроблено в рамках проекту OWASP, а саме OWASP ZAP. Такий вибір обумовлено простотою використання й значною поширеністю цього програмного забезпечення серед фахівців з кібербезпеки.

Для проведення експерименту з визначення вразливостей веб-сайтів закладів вищої освіти обрали шість університетів:

1) Донецький національний університет імені Василя Стуса (Вінниця),
2) Національний університет «Львівська політехніка» (Львів),
3) Київський політехнічний інститут імені Ігоря Сікорського (Київ),
4) Харківський національний університет радіоелектроніки (Харків),
5) Одеський національний політехнічний університет (Одеса),
6) Український католицький університет (Львів).

Вибір обумовлено такими чинниками: перша позиція – альма-матер автора статті, позиції з другої по п'яту обрано як одні з найбільших університетів за географічним принципом, шосту позицію внесено як найпотужніший представник приватного університету.

Результати сканування наведено в таблиці 1.

Таблиця 1

Результати сканування веб-сайтів провідних закладів вищої освіти України

Тип вразливості	ДонНУ	ЛП	КПІ	ХНУРЕ	ОНПУ	УКУ
1	2	3	4	5	6	7
X-Frame-Options Header Not Set	+	+	+	+	+	+
Absence of Anti-CSRF Tokens	+	+	+	+	+	+
Application Error Disclosure			+			
Cookie No HttpOnly Flag	+		+	+		+
Cookie Without Secure Flag	+			+		+
Cross-Domain JavaScript Source File Inclusion		+	+	+	+	+
Incomplete or No Cache-control and Pragma HTTP Header Set	+		+	+		+

1	2	3	4	5	6	7
Information Disclosure - Debug Error Messages			+			
Private IP Disclosure	+				+	
Secure Pages Include Mixed Content	+		+	+		
Web Browser XSS Protection Not Enabled	+	+	+	+	+	+
X-Content-Type-Options Header Missing	+	+	+	+	+	+

Якщо вважати, що за половини чи більше випадків наявності відповідної вразливості така вразливість є характерною, можна зменшити їх коло (таблиця 2).

Таблиця 2

Зміст вразливостей, які становлять поверхню атаки для веб-сайту закладу вищої освіти

Тип вразливості	Ризик використання	Опис вразливості
1	2	3
X-Frame-Options Header Not Set	Середній	Сервер не повернув заголовка параметрів X-Frame, це означає, що такому веб-сайту може загрожувати атака типу clickjacking. Clickjacking (User Interface redress attack, UI redress attack, UI redressing) – тип атаки, який призводить до натискання користувачем іншого об'єкта
Absence of Anti-CSRF Tokens	Середній	Веб-додаток не дає змоги чи не може в достатній мірі перевірити, чи було навмисно надано добре сформований, дійсний, послідовний запит користувачем, який подав запит
Cookie No HttpOnly Flag	Середній	Якщо файл cookie встановлено з прапором HttpOnly, він вказує браузеру, що доступ до файла cookie може здійснювати тільки сервер, а не скрипти на боці клієнта
Cross-Domain JavaScript Source File Inclusion	Середній	Веб-сайт імпортує або містить виконувану функційність (наприклад, бібліотеку) з джерела, яке міститься поза передбачуваною сферою керування
Incomplete or No Cache-control and Pragma HTTP Header Set	Середній	Для кожної веб-сторінки сайт повинен мати відповідну політику кешування, яка визначає ступінь кешування сторінки та її форм
Web Browser XSS Protection Not Enabled	Середній	Заголовок відповіді HTTP X-XSS-захисту дає змогу веб-серверу вмикати або вимикати механізм захисту XSS веб-браузера
X-Content-Type-Options Header Missing	Середній	Відсутність налаштувань заголовка для параметрів типу X-Content, це означає, що він вразливий до MIME sniffing, що може бути використано для атаки типу Cross-Site Scripting (XSS). Cross-Site Scripting (XSS) – це тип ін'єкції, за якого зловмисні скрипти (сценарії) впроваджують на надійні веб-сайти

Не зупинятимемося докладно на цих вразливостях, проте інформацію щодо специфіки перелічених вище вразливостей та методів боротьби з ними можна дізнатися, наприклад, на ресурсі https://cwe.mitre.org/.

Процес тестування на проникнення

З усього наведеного вище можна запропонувати таку структуру процесу тестування на проникнення веб-сайту закладу вищої освіти на відповідних етапах запропонованої раніше методології (рис. 1).

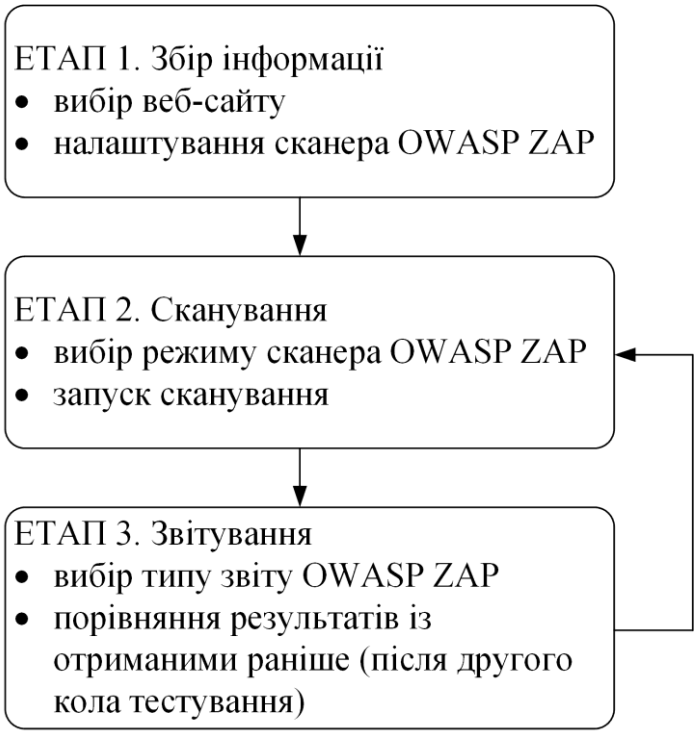

Рисунок 1. Процес проведення тестування на проникнення

За першого сканування під час налаштування OWASP ZAP треба обмежити типи вразливостей для сканування відповідно до виділених вище. Якщо одну або кілька можливих вразливостей виявлено, приймають рішення щодо їх виправлення. За умови прийняття рішення про виправлення після проведених змін проводять повторне сканування й порівняння результатів.

Висновки. Забезпечення контролю кіберзахисту веб-сайту в закладах вищої освіти зазвичай має несистемний характер, тому запропонована в праці методологія тестування на проникнення мала на меті об'єднати два аспекти. По-перше, вона досить проста й складається всього з трьох етапів (перший – збирання інформації та її аналізування; другий – тестування керування конфігурацією та тестування керування сесіями; третій – звітування й переведення системи в початковий стан). По-друге, для скорочення часу на проведення першого етапу в налаштуваннях сканера вразливостей (у праці пропонують використовувати OWASP ZAP), як засвідчили дослідження на вразливості веб-сайтів провідних університетів України, треба сконцентруватися на таких вразливостях, як X-Frame-Options Header Not Set, Absence of Anti-CSRF Tokens, Cookie No HttpOnly Flag, Cross-Domain JavaScript Source File Inclusion, Incomplete or No Cache-control and Pragma HTTP Header Set, Web Browser XSS Protection Not Enabled та X-Content-Type-Options Header Missing.

ЛІТЕРАТУРА

1. Oriyano Sean-Philip Penetration testing essentials. *Indianapolis: John Wiley & Sons, Inc.* 2017. 349 p.
2. Bertoglio D. D., Zorzo A. F. Overview and open issues on penetration test. *Journal of the Brazilian Computer Society*. 2017. №23. P. 1–16.
3. Halton W., Weaver B., Ansari J. A. Penetration Testing: A Survival Guide. *Birmingham: Packt Publishing Ltd.* 2016. 1045 p.
4. Mohit R. Python Penetration Testing Essentials. *Birmingham: Packt Publishing Ltd*. 2015. 178 p.
5. Mirjalili M., Nowroozi A., Alidoosti M. A survey on web penetration test. *Advances in Computer Science: an International Journal*. 2014. № 3. P. 107–121.
6. Phong C. T. A Study of Penetration Testing Tools and Approaches. Master thesis of Computer and Information Sciences. *Auckland University of Technology*. 2014. 125 p.
7. Shanley A., Johnstone M. N. Selection of penetration testing methodologies: A comparison and evaluation. *The Proceedings of [the] 13th Australian Information Security Management Conference*. 2015. P. 65–72.
8. Kang Y.-S., Cho H.-H., Shin Y. and Kim J.-B. Comparative Study of Penetration Test Methods. *Advanced Science and Technology Letters*. 2015. Vol.87. P. 34–37.
9. Порошин С. М., Можаєв О. О., Можаєв М. О. Методологія проведення pen-тестування веб-додатків. *Системи обробки інформації*. 2016. Випуск 3 (140). С. 33–35
10. Patel Y., Sheth R. Web Services Pen-testing Framework for Cyber Security : A Review. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 2017. Volume 2, Issue 6. P. 306–308.
11. Барибін О. І. Сучасні методології тестування на проникнення. *Кібербезпека у системі національної безпеки України: пріоритетні напрями розвитку: збірник матеріалів наукового круглого столу, м. Маріуполь, 26 квітня 2018 р*. С. 63–66.
12. OWASP Top 10 –2017. The Ten Most Critical Web Application Security Risks. *Creative Commons (CC) Attribution Share-Alike*. 2017. 25 p.
13. Meucci V. and Muller A. OWASP Testing guide 4.0 release. *Creative Commons (CC) Attribution Share-Alike*. 2016. 224 p.

Барыбин А. И.

МЕТОДОЛОГИЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ ВЕБ-САЙТА ВЫСШЕГО УЧЕБНОГО ЗАВЕДЕНИЯ

В статье рассмотрена проблема контроля качества киберзащиты сайта высшего учебного заведения путем использования технологий тестирования на проникновение. На основе анализа современных методологий тестирования на проникновение предложена методология, состоящая из трех этапов (первый – сбор информации и ее анализ, второй – тестирование управления конфигурацией и тестирование управления сессиями, третий – формирование отчета и перевод системы в исходное состояние). Результаты исследований типичных уязвимостей для сайтов университетов Украины позволили ограничить возможную поверхность атаки, что ускорит поиск и анализ уязвимостей на первом этапе предлагаемой методологии.

Ключевые слова: *тестирование на проникновение, веб-сайт, OWASP, OWASP ZAP.*

Barybin O.

AGILE SOFTWARE DEVELOPMENT METHODOLOGY SCRUM QUALITY MODEL

The article considers the problem of quality control of a higher educational institution website cybersecurity by using penetration testing technologies. Based on an analysis of modern penetration testing methodologies, a three-stage methodology is proposed (1 collecting and analyzing information, 2 testing configuration management and testing session management, 3 generating a report and resetting the system). The results of studies of typical vulnerabilities for

Ukrainian universities web-sites made it possible to limit the possible attack surface, which would speed up the search and analysis of vulnerabilities at the first stage of the proposed methodology.

Key words: *penetration testing, web-site, OWASP, OWASP ZAP.*

Рецензент: Фурса С. Є., канд. техн. наук, доцент, Донецький національний університет імені Василя Стуса, м. Вінниця

UDC 661.94/66.021.1

Rozbytska T., Sukhenko V., Miedviedieva N.

THE EFFECTIVE WASTEWATER TREATMENT FOOD PROCESSING AND AGRIBUSINESS

The proposed sewage treatment process using ozone carried out in bubblers in countercurrent motion of phases.

Key words: Ozone, phase, the apparatus, the intensification, the process.

Formulation of the problem. In the processing industries of the agro-industrial complex, where in the cost of production the share of material and energy costs is more than 80%, the importance of reducing the material consumption becomes especially urgent. This can be achieved thanks to the wide introduction of non-waste technologies, the integrated use of raw materials and secondary resources in combined production. Another important aspect of the problem is ensuring the ecological safety of food production plants, eliminating the harmful effects of waste on the environment. The food industry belongs to the most material-intensive industries, therefore the rational use of raw materials is especially important. The problem of waste disposal is one of the most important issues faced by food industry enterprises.

Every year the pollution of the natural environment increases. Food processing and agribusiness companies by its emissions significantly affect the water environment and air.

Analysis of recent research and publications. Famous domestic and foreign scientists have devoted considerable attention to research on the effective treatment of water from processing and food enterprises. However, despite the presence of a large number of scientific studies on this issue, some aspects of modern sewage treatment using ozone are still not well-researched, which have an important scientific-theoretical value and practical value.

The purpose of the article. To estimate the state of sewage of processing and food industries, and the proposed sewage treatment process using ozone carried out in bubblers in countercurrent motion of phases.

Presentation of the main research material. A promising method of water treatment is an ozonation. Ozone eliminates bad tastes and odors, oxidize soluble organic compounds and provides a fast and reliable disinfection and improves organoleptic properties of water. The ozone promotes oxidation and causes the precipitation of iron and manganese, precluding the colour of water.

Thus, the universal nature of ozone makes it promising for water treatment and sewage treatment of the enterprises of processing and food industry. However, the wide practical use of ozone is constrained by insufficient study of the process and the lack of high performance of the