УДК 004(9+056.53)

О.І. Міснік, Київ
М.В. Антонішин, Київ
В.В. Цуркан, Київ

АНАЛІЗ ЯКОСТІ РОБОТИ СКАНЕРІВ УРАЗЛИВОСТЕЙ ВЕБ-ЗАСТОСУНКІВ

Abstract. The main objective of this work was to find out the effectiveness of Zaproxy, W3AF, Arachni an open source and free integrated penetration testing tool for finding vulnerabilities in web applications. For this project, web application with vulnerability were used as tools, PHP, HTML, JavaScript, C#, Python and CSS as languages, and MySQL and MSSQL Database for making a prototype web application. Zaproxy, W3AF, Arachni were used as a testing tools. The reason for using Zaproxy, W3AF, Arachni are that it is an open source and free applications and it is a very popular tools among all available web application penetration testing tools either commercial or open source. Some vulnerabilities were successfully found by the application. To test the effectiveness of Zaproxy, W3AF, Arachni in more detail was own making practice experiment.

Вступ

Нині веб-безпека набуває популярності і використання веб-сканерів стало основним інструментом виявлення уразливостей при оцінюванні стану захищеності веб-застосунків. Оскільки оцінювання стану захищеності здійснюється за допомогою веб-сканерів уразливостей, то виникає потреба в аналізуванні якості їх роботи. Якість є головним критерієм їх використання і тлумачиться як кількість виявлених уразливостей. Однак, це не та кількість, яка заявлена виробником, а та, яку насправді веб-сканер може виявити. Тому в статті розглядаються відкриті інструменти пошуку уразливостей веб-застосунків. Проводиться тестування роботи веб-сканерів та досліджується придатність інструменту стосовно якісного вирішення поставленого перед ним завдання. Для більш детального узагальнення результатів тестування веб-сканерів проведено на веб-застосунках, які розроблено за допомогою різних технологій. Це дозволяє краще проаналізувати якість роботи даного різновиду програмного забезпечення.

Аналіз останніх досліджень і публікацій

За результатами аналізування джерел [1 – 5] встановлено, що тема якості роботи веб-сканерів уразливостей розкрита недостатньо. Зокрема, при проведені досліджень веб-застосунків, які розроблені різними мовами програмування та використовують різні технології для функціонування.

Мета

Проаналізувати якість роботи сканерів виявлення уразливостей веб-застосунків.

Основна частина

В останній час наявність уразливостей веб-застосунків призводять до компрометації конфіденційної інформації, тому цим питання зацікавилися на державному рівні і, як наслідок, видано Наказ Адміністрації Держспецзв'язку від 15.01.2016 № 20 «Про затвердження Порядку сканування на предмет уразливості державних інформаційних ресурсів, розміщених в Інтернеті» [1]. Даний наказ описує, що сканування є важливим етапом виявлення уразливостей веб-застосунків. Для їх сканування використовуються веб-сканери, але на практиці виконання цього завдання обмежується декількома аспектами. По-перше, немає чіткого переліку уразливостей, які потрібно шукати при проведенні сканування, а, по-друге, немає переліку актуального програмного забезпечення для динамічного аналізування веб-застосунків. Якщо перелік основних уразливостей веб-застосунків є, наприклад, у OWASP TOP 10 (мета проекту – підвищення інформованості про існуючі та найбільш розповсюджені уразливості веб-застосунків) [2]. На даний перелік існує посилання у багатьох стандартах, інструментах і настановах, включаючи MITRE, PCI DSS, DISA, FTC. Нині доступна версія release candidate 2017 року. Однак, переліку актуального програмного забезпечення для сканування веб-застосунків з актуальними результатами досліджень їх переваг та недоліків немає.

Тому спочатку опишемо, що таке веб-сканер уразливостей. Це програма, яка взаємодіє з веб-застосунком через веб-інтерфейс для виявлення потенційних уразливостей та архітектурних слабких сторін [3]. Вона дозволяє перевіряти веб-застосунки на предмет наявності уразливостей, якими можуть скористатися зловмисники.

При виборі умов порівняння за основу взято підхід "від завдань". Таким чином, за результатами такого порівняння можна судити, наскільки той чи інший інструмент придатний для вирішення поставленого перед ним завдання. Наприклад, веб-сканери безпеки можуть бути використані при оцінюванні захищеності, тестуванні на проникнення та для перевірки відповідності веб-застосунків аудиторським вимогам.

Алгоритм роботи сканерів залишається незмінним та складається з таких етапів [1]:

1. Збирання інформації про веб-застосунок. На даному етапі ідентифікуються всі можливі запити до нього та знаходяться всі можливі точки входу.

2. Виявлення потенційних уразливостей. Сканер використовує базу уразливостей для перевірки веб-застосунку на наявність уразливостей.

3. Підтвердження виявлених уразливостей. Сканер використовує спеціальні методи і моделює атаки для підтвердження факту наявності

уразливостей.

4. Генерування звітів. На основі зібраної інформації система аналізування захищеності створює звіти, що описують виявлені уразливості.

Для вибору веб-сканерів, потрібно спочатку визначити серед них актуальні на даний момент. Тобто якщо веб-сканер протягом останнього року не оновлювався, то такий веб-сканер складно вважати актуальним.Тому одним з основних параметрів відбору є дата оновлення веб-сканеру уразливостей [6], а також належність до списку програмного забезпечення з відкритим кодом.

Проаналізувавши останні дати оновлення веб-сканерів, можна зробити висновок, що актуальними веб-сканерами є Zaproxy, w3af та Arachni. Ці веб-сканери з великою функціональністю і відкритим кодом володіють зрозумілим користувацьким інтерфейсом, а також мають низький поріг входу для початку використання і не вимогливі до досвіду тестування безпеки веб-застосунків. Дані сканери працюють автоматично, тобто не потребують втручання людини окрім вводу потрібного для сканування домену. Це дозволяє проводити тестування без глибоких знань про уразливості веб-застосунків. Перелічені веб-сканери досить популярні, однак аналіз їх результатів сканування веб-застосунків, розроблених за допомогою різних мов програмування на даний момент проведено не було.

Методика порівняння веб-сканерів. Поетапно проаналізовано роботу веб-сканерів на веб-застосунках, використовуючи їх функціонал пошуку уразливостей. Після аналізування звітів зі знайденими уразливостями та маючи інформацію про кількість уразливостей веб-застосунків буде виявлено який веб-сканер більш якісно працює під час пошуку вразливостей.

Для даного експерименту використовуються спеціалізовані відкриті веб-застосунки, які призначені для тестування програмного забезпечення стосовно наявності вразливостей. Тому у табл. 1 наведено перелік веб-застосунків, які використовувалися для тестування, а також перелік технологій їх розроблення [11].

Таблиця 1

Перелік веб-застосунків для тестування

Веб-застосунок	Уніфікований локатор ресурсів	Технології
Security Tweets	http://testhtml5.vulnweb.com	nginx, Python, Flask, CouchDB
Acuart	http://testphp.vulnweb.com	Apache, PHP, MySQL
Acublog	http://testaspnet.vulnweb.com	IIS, .NET, Microsoft SQL Server

Якість пошуку уразливостей оцінюється в балах за наступною схемою. Кожна уразливість матиме свою оцінку, тобто при знаходженні критичної уразливості додаємо 3 бали, при знаходженні високої – 2 бали, середньої уразливості – 1 бал, а при знаходженні низької – 0.5 бала.

Для визначення рівня уразливості потрібно знати ознаки за якими їх можна охарактеризувати. Опис рівнів уразливостей взято для CVSS v3 Atlassian, яка використовує таку систему оцінки уразливостей [13]:

Рівень уразливості – критичний. Уразливості, які належать критичному діапазону, як правило, мають більшість з наступних характеристик:

- використання уразливості, ймовірно, призведе до компрометації серверів або інфраструктурних пристроїв на кореневому рівні;
- експлуатація звичайно проста, в тому сенсі, що зловмиснику не потрібні спеціальні автентифікаційні облікові дані або знання про об'єкт нападу, і не потрібно переконувати цільового користувача, наприклад, через соціальну інженерію, у виконанні будь-яких спеціальних функцій.

Рівень важкості – високий. Уразливості, які мають високий рівень, зазвичай мають деякі з таких характеристик:

- уразливість важко експлуатувати;
- експлуатація може призвести до підвищення привілеїв;
- експлуатація може призвести до значної втрати даних або простоїв роботи.

Рівень важкості – середній. Уразливості, які належать середньому діапазону, зазвичай мають деякі з таких характеристик:

- уразливості, які вимагають від зловмисника маніпулювати окремими "жертвами" через використання соціальної інженерії;
- атака на відмову в обслуговуванні, тобто напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена;
- дії, які вимагають від зловмисника перебувати в тій самій локальній мережі, що й "жертва".
- уразливості,експлуатація яких забезпечує дуже обмежений доступ.
- уразливості, які потребують користувацьких привілеїв для успішної експлуатації.

Рівень важкості – низький. Уразливості в низькому діапазоні, як правило, дуже мало впливають на організацію. Експлуатація таких уразливостей зазвичай вимагає доступу до локальної або фізичної системи.

Експеримент 1. У табл. 2 наведено перелік усіх наявних уразливостей веб-застосунку для тестування Security Tweets та вказана кількість уразливостей, які насправді знайдено при тестуванні даного веб-застосунку.

Таблиця 2

Результати тестування Security Tweets

Перелік уразливостей додатку	Кількість уразливостей	Веб-сканери			Рівень уразл.-ті
		W3AF	Arachni	Zaproxy	
AngularJS client-side template injection	1				Високий
DOM-based cross site scripting	3		1		
nginx SPDY heap buffer overflow	1				
Weak password / broke auth function	1				
Basic authentication over HTTP	1				Середній
HTML form without CSRF protection	1		1		
User credentials are sent in clear text	1	1	1		
Vulnerable Javascript library	1				Низький
Clickjacking: X-Frame-Options header missing	1	1	1	1	
Cookie(s) without HttpOnly flag set	1		1	1	
OPTIONS method is enabled	1				
Login page password-guessing attack	1		1	1	
Possible sensitive directories	3		3		
Загальна кількість балів	31	1.5	7	1.5	

З табл. 2 бачимо, що найкраще себе показав веб-сканер Arachni з найбільшою кількістю балів. Тоді як сканери Zaproxy та w3af показали слабку результативність.

Експеримент 2. У табл. 3 наведено перелік наявних уразливостей веб-застосунку для тестування Acuart та вказано кількість уразливостей, які було насправді знайдено при його тестуванні.

Таблиця 3

Результати тестування Acuart

Перелік уразливостей додатка	Кількість уразливостей	Перелік сканерів уразливостей			Рівень уразл.-ті
		W3AF	Arachni	Zaproxy	
Blind SQL Injection	1		1	1	Критичний
File inclusion	1	1	1		
Remote file inclusion	1	1			
SQL injection	11	8	2	6	
Cross site scripting	16	10	16	14	Високий
nginx SPDY heap buffer overflow	1				
Macromedia Dreamweaver remote database scripts	1				
Script source code disclosure	1				
Weak password	1				
Application error message	5				Середній
Backup files	2		2		
CRLF injection/HTTP response splitting	1				
Cross domain data hijacking	1			1	
Cross site scripting (content-sniffing)	1				
Directory listing	10				
Error message on page	1				
.htaccess file readable	1				
HTML form without CSRF protection	6				
HTTP parameter pollution	1				
Insecure crossdomain.xml file	1		1		
JetBrains .idea project directory	1				

Source code disclosure	2				
URL redirection	1				
User credentials are sent in clear text	2		2		
WS_FTP log file found	1				Низький
Clickjacking: X-Frame-Options header missing	1	1	1	1	
Hidden form input named price was found	1				
Login page password-guessing attack	1	1	1		
Possible sensitive directories	3		3		
Possible sensitive directories	2				
Cookie(s) without HttpOnly flag set	1	1		1	
Загальна кількість балів	123	51.5	51.5	51	

В даному випадку бачимо, що всі веб-сканери показали майже однаковий результат, отримавши майже однакову кількість балів.

Експеримент 3. У табл. 4 також наведено перелік наявних уразливостей веб-застосунку для тестування Acublog та вказана кількість уразливостей, які насправді знайдено при його тестуванні.

Таблиця 4

Результати тестування Acublog

Перелік уразливостей додатка	**Кількість уразливостей**	**Перелік сканерів уразливостей**			**Рівень уразл.-ті**
		W3AF	**Arachni**	**Zaproxy**	
Blind SQL Injection	2	2	1	1	Критичний
Cross site scripting	1	1	1	1	Високий
Microsoft IIS tilde directory enumeration	1				
User controllable script source	1				

Application error message	2				Середній
ASP.NET error message	1				
Cross frame scripting	1				
Unencrypted __VIEWSTATE parameter	7				
User credentials are sent in clear text	1		1		
ASP.NET debugging enabled	1				
Clickjacking: X-Frame-Options header missing	1		1	1	Низький
Login page password-guessing attack	1		1		
OPTIONS method is enabled	1				
Possible relative path overwrite	4				
Possible sensitive directories	2				
Загальна кількість балів	29.5	9	7	5.5	

За табл. 4 бачимо, що всі веб-сканери показали майже однаковий результат, отримавши майже однакову кількість балів.

Після проведених експериментів можемо підбити загальну кількість отриманих балів.

Назва веб-застосунку	Загальна кількість балів	W3AF	Arachni	Zaproxy
Security Tweets	31	1.5	7	1.5
Acuart	123	51.5	51.5	51
Acublog	29.5	9	7	5.5

Висновки

- проаналізувавши результати сканувань можемо зробити висновок, що найкраще себе проявив веб-сканер Arachni. Тоді як інші проявили себе на одному рівні.

- при аналізуванні результатів експерименту бачимо, що веб-сканери мають найкращу якість при тестуванні веб-застосунків, які розроблені за допомогою мови програмування PHP. Однак, при тестуванні інших веб-застосунків маємо велику кількість не виявлених уразливостей, тобто в даному випадку використання тільки веб-сканерів не доцільне.
- встановлено, що веб-сканери є неоднозначним інструментом виявлення уразливостей і не дають остаточних гарантій безпеки веб-застосунків.

У перспективі подальших досліджень планується розширити проведення експерименту з виявлення уразливостей веб-застосунків шляхом використання систем виявлення вторгнень та файєрволів.

1. *Рожкова Екатерина Олеговна, Ильин Иван Валерьевич, Галушин Сергей Яковлевич*. Обзор и сравнение сканеров уязвимостей (2015). Электронный сборник статей по материалам XXX студенческой международной заочной научно-практической конференции ISSN 2310-4066.
2. *Priyank Bhojak, Vatsal Shah, Kanu Patel, Deven Gol.* Automated Web Application Vulnerability Detection With Penetration Testing (2017). Kalpa Publications in Computing. ICRISET 2017. International Conference on Research and Innovations in Science, Engineer-
ing & Technology. Selected Papers in Computing.
3. *Marco Vieira, Nuno Antunes, Henrique Madeira*. Using Web Security Scanners to Detect Vulnerabilities in Web Services (2009). Faculty of sciences and technologies university of Coimbra.
4. *О.Р. Лапонина, С.А. Малаховский* – Использование сканера уязвимостей ZAP для тестирования веб-приложений. International Journal of Open Information Technologies ISSN: 2307-8162 – 2017
5. OWASP Zed Attack Proxy Project [Електронний ресурс] – Режим доступу: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project – Назва з екрану
6. Наказ Адміністрації Держспецзв'язку від 15.01.2016 № 20 «Про затвердження Порядку сканування на предмет уразливості державних інформаційних ресурсів, розміщених в Інтернеті», який зареєстровано в Міністерстві юстиції України 05.02.2016 за № 196/28326 [Електронний ресурс] – Режим доступу: http://zakon3.rada.gov.ua/laws/show/z0196-16 – Назва з екрану
7. OWASP Top 10 https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project [Электронный ресурс] – Режим доступу: https://www.owasp.org/index.php/Category: OWASP_Top_Ten_Project – Назва з екрану.
Web application security scanner [Электронный ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Web_application_security_scanner – Назва з екрану.
8. The Attack Vectors Supported by Web Application Scanners [Електронний ресурс] – Режим доступу: http://www.sectoolmarket.com/ – Назва з екрану.
9. Category:Vulnerability Scanning Tools [Электронный ресурс] – Режим доступу: https://www.owasp.org/index.php/Category:Vulnerability_Scanning_ Tools – Назва з екрану.
10. List of vulnerable test websites [Електронний ресурс] – Режим доступу: http://www.vulnweb.com – Назва з екрану
11. Веб-сканер w3af [Електронний ресурс] – Режим доступу: http://w3af.org – Назва з екрану.

12. Веб-сканер arachni [Електронний ресурс] – Режим доступу: http://www.arachni-scanner.com – Назва з екрану.
13. Severity Levels for Security Issues [Електронний ресурс] – Режим доступу: https://www.atlassian.com/trust/security/security-severity-levels – Назва з екрану.

Поступила 5.02.2018р.

УДК 519.711

А.Л. Березкін, Київ

ПРОГРАМНО ВИЗНАЧАЄМЕ РАДІО – СУЧАСНІ ТЕХНОЛОГІЇ МОДЕЛЮВАННЯ ТА КОНСТРУЮВАННЯ РАДІОПРИСТРОЇВ

Abstract. The scientific and technical prerequisites for the emergence of SDR technology are considered. Its application at present, prospects for development. The possibilities of using SDR software platforms for the development of computer simulation of signal processing processes.

Актуальність

Стрімке технологічне зростання людства за останні 10-15 років поставило питання про чергову індустріальну революцію Industria-4.0. І як що час між першими трьома індустріальними революціями сягав десятиліття, то час між третьою (кінець 80-х, початок 90-х років) та четвертою пройшов менше за життя одного покоління.

Основними рисами двох останніх індустріальних революцій є те, що вони пов'язані з цифровими технологіями. Третя індустріальна революція –це проникнення цифрових технологій в усі галузі техніки. Четверта індустріальна революція – інформаційна, характеризується проникненням і у суспільні відносини, змінюючи їх традиційне значення. З'являються нові напрямки відносин, таки як IoT, що характеризуються тим, що стирають межи між суспільними і технічними відносинами людства.

В роботах [5-7] позначені напрямок розвитку сучасних технологій, що характеризуються тісним сплетінням технологій, як радіо, цифрова обробка, комп'ютерні технології, обробка інформації.

Однією із знов створених технологій, яка є невід'ємною частиною Industria-4.0, являється програмно визначаєме радіо ПВР (англійською SoftDefineRadio – SDR).

Постановка задачі

Щоб дотримуватись міжнародної термінології, ПВР будемо називати SoftDefineRadio(SDR). Для більш стислої подачі матеріалу у статті, роздивимось тільки прийомну частину радіопристроїв, яка, зазвичай, є більш

