ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет
радіоелектроніки
Кафедра ЕОМ

МЕТОДИ ТА ЗАСОБИ ОЦІНКИ ЗАХИЩЕНОСТІ САЙТІВ

Кваліфікаційна робота
Другий (магістерський) рівень

Автор :
Сорокін В. О.
студ. гр. СПзм - 20 - 1

Керівник :
Федорченко В. М.
к. т. н, доц. каф. ЕОМ

1

Об’єкт, мета та завдання

- Об’єктом дослідження є процес функціонування веб-застосувань
- Предметом дослідження є захищеність веб-застосувань.
- Метою є підвищення захищеності веб-застосувань.

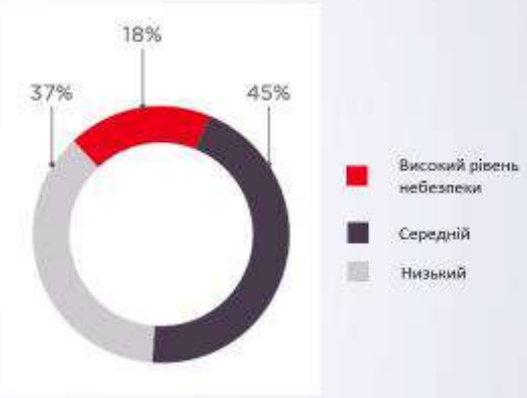
Завданнями роботи є:

- Аналіз сучасних проблем веб-застосувань стосовно їх безпеки.
- Аналіз методологій тестування захищеності веб-застосувань.
- Аналіз інструментів для пошуку вразливостей.
- Тестування веб-застосування на безпеку, й оцінка його захищеності.

2

Сучасні проблеми захищеності веб-застосувань

Згідно аналізу захищеності веб застосуваньдоля вразливих веб-додатків становить 83%.

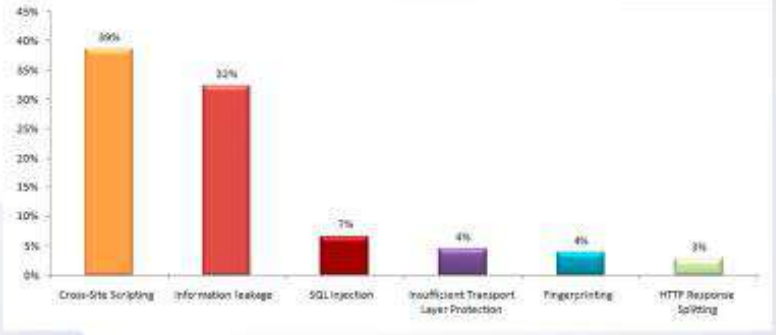


Кількість вразливостей, в залежності від рівня їхньої небезпеки.

3

Найпоширеніші вразливості

Кількість вразливостей у веб-застосуваннях



4

Найпоширеніші вразливості

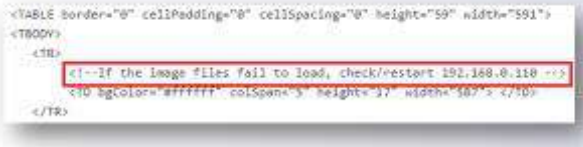
XSS (Cross-Site Scripting) – це вид вразливості, при якому на генерованій сервером сторінці, виконуються шкідливі скрипти з метою атаки клієнта.

Приклади шкідливих скриптів:

```
<script>alert(document.cookie);</script>
<script>window.parent.location.href='http://hacker_site';</script>
```

Information Leakage (Витік інформації) – це категорія вразливостей, в якій інформація ненавмисно розкривається кінцевим користувачам.

Приклад витоку інформації:



5

Найпоширеніші вразливості

Code injections (SQL, PHP, ASP и т. д.) – це вид уразливості, коли запускається шкідливий код одночасно з основним виконуваним кодом, з метою отримання доступу до системних ресурсів, несанкціонованого доступу до даних або узагалі виведення системи з ладу.

Приклад SQL ін'єкції:

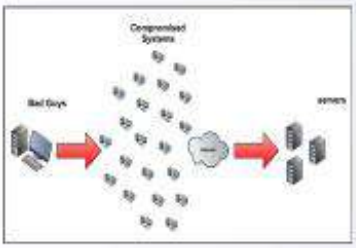
```
SELECT Username
FROM Users
WHERE Name = 'tester'
AND Password = 'testpass' OR '1'='1';
```

Insufficient Transport Layer Protection (Недостатній захист транспортного рівня) – дозволяє обмінюватися даними з ненадійними третіми сторонами, що призводить до крадіжки конфіденційної інформації.

6

Найпоширеніші вразливості

DoS-атака – це напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена.



7

Методології тестування захищеності веб-застосувань

При тестуванні на безпеку перевірці підлягає наступне:

- контроль доступу – визначає проблеми, пов'язані з несанкціонованим доступом користувачів до інформації та функцій в залежності від наданої ролі;
- аутентифікація – дозволяє упевнитися у відсутності можливості обійти процедуру реєстрації та авторизації; переконатися в коректності управління призначеними для користувача даними, виключити можливість отримання інформації про зареєстрованих користувачів і їх облікових даних;
- затвердження вхідних значень – використовується для перевірки алгоритмів обробки даних, включаючи некоректні значення, перш, ніж на них буде посилатися додаток;
- криптографія – виявляє проблеми, пов'язані з шифруванням, дешифруванням, підписом, верифікацією достовірності, в тому числі включаючи рівень мережевих протоколів, роботу з тимчасовим файлами і cookies;
- механізми обробки помилок – включає перевірку системних помилок додатку на відсутність факту розкриття інформації про внутрішні механізми безпеки;
- інтеграція зі сторонніми сервісами – дозволяє переконатися в неможливості маніпуляції даними, переданими між додатком і сторонніми компонентами, наприклад, платіжними системами або соцмережами;
- перевірка стійкості до Dos та DDos атак – перевіряє здатність додатку обробляти незаплановано високі навантаження і великі обсяги даних, які можуть бути спрямовані на виведення додатку з ладу

Також важливим етапом тестування сайту є тестування продуктивності (Performance testing)

8

Методології тестування захищеності веб-застосувань

Принципи тестування, які ми можемо використати:

- DAST (Dynamic Application Security Testing) – динамічний (тобто вимагає виконання) аналіз додатку без доступу до вихідного коду і серверної частини;
- SAST (Static Application Security Testing) – статичний (тобто не вимагає виконання) аналіз додатку з доступом до вихідного коду і до веб-сервера, по суті це аналіз вихідного коду за формальними ознаками наявності вразливостей і аудит безпеки сервера;
- IAST (Interactive Application Security Testing) – динамічний аналіз безпеки веб-додатку, з повним доступом до вихідного коду та веб-сервера;
- аналіз вихідного коду – статичний або динамічний аналіз з доступом до вихідного коду без доступу до серверного оточення

9

Методології тестування захищеності веб-застосувань

OWASP (Open Web Application Security Project) – це некомерційна організація, метою якої є підвищення обізнаності всіх фахівців галузі інформаційної безпеки в питаннях розробки, експлуатації та захисту веб-додатків.

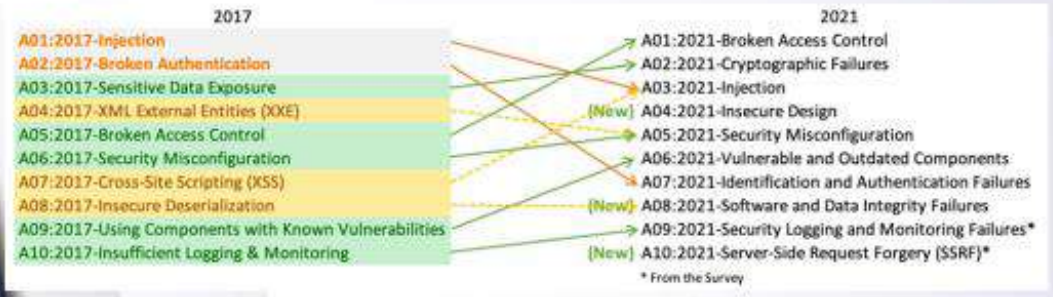
OWASP Top 10 – це рейтинг з десяти найбільш небезпечних ризиків інформаційної безпеки для веб-додатків, складений спільнотою експертів галузі.

№	Назва
1	Ін'єкції
2	Некоректна аутентифікація
3	Витік конфіденційних даних
4	Зовнішні XML-сутності (XXE)
5	Порушення контролю доступу
6	Помилки в налаштуваннях безпеки
7	Міжсайтовий скриптинг
8	Небезпечна десеріалізація
9	Використання компонентів з відомими вразливостями
10	Недоліки ведення журналу та моніторингу

10

Методології тестування захищеності веб-застосувань

З 2011 року OWASP випускає рейтинг Top 10 Mobile Risks, який постійно оновлюється



11

Методології тестування захищеності веб-застосувань

CWE (Common Weakness Enumeration) – загальний перелік вразливостей і недоліків безпеки програмного забезпечення, являє собою ієрархічний словник, призначений для розробників і фахівців щодо забезпечення безпеки програмного забезпечення.

Для класифікації недоліків використовується багаторівнева структура, яка описує деревоподібний пристрій CWE: кінцеві недоліки об'єднуються в типи, типи - в категорії, категорії – в представлення. Кожне представлення –особливий спосіб класифікації записів CWE, призначений для спрощення вирішення конкретного завдання.

12

Методології тестування захищеності веб-застосувань

WASC (The Web Application Security Consortium) – це некомерційна організація, яка раніше активно займалася розробкою і просуванням стандартів безпеки додатків.

Атаки і недоліки в проекті сформовані в два представлення: перше – це простий перелік, а друге – це розподіл по трьох етапах розробки (проектування, реалізація, впровадження). Всього в списках описано 34 типи атак і 15 типів недоліків.

13

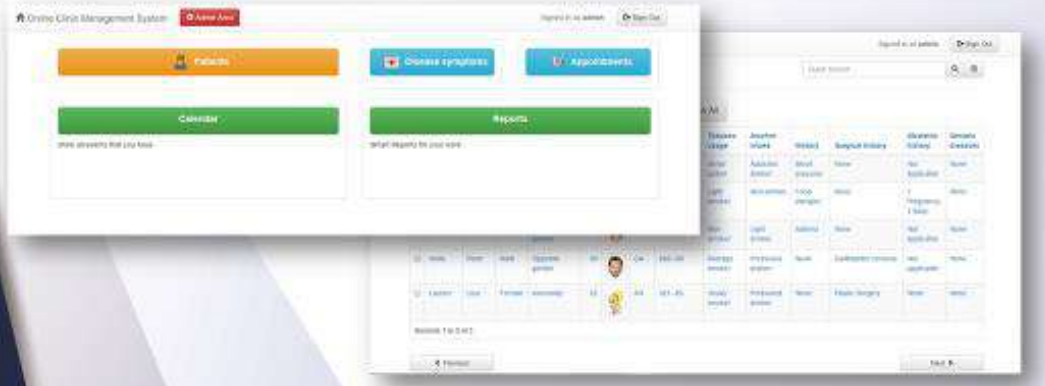
Послідовність виконання роботи

- Аналіз веб-застосування, обраного для дослідження;
- Вибір інструментів для пошуку вразливостей;
- Пошук вразливостей й оцінка рівня небезпеки кожної з них;
- Розрахунок оцінки захищеності даного веб-застосування.

14

Веб-застосування для дослідження

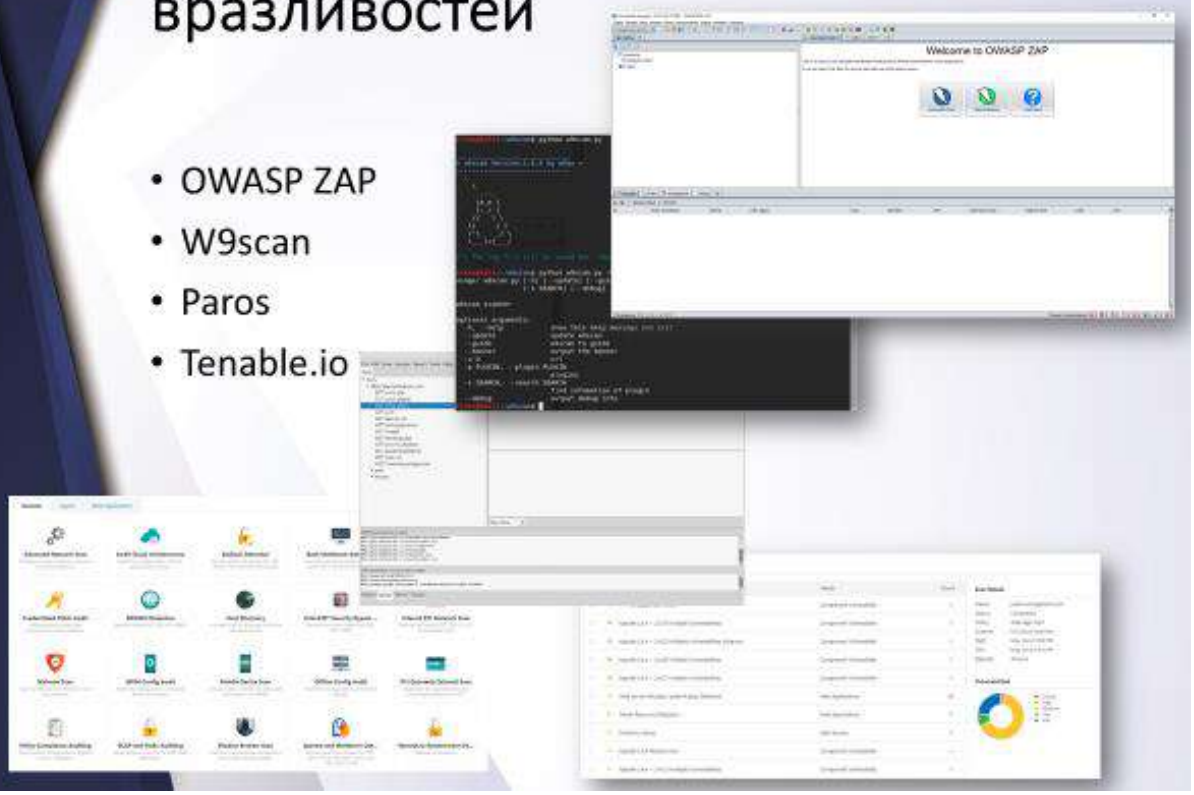
Для дослідження було обрано онлайн-систему управління клінікою. Ця програма дає змогу спостерігати за діяльністю клініки і зберігає історію кожного пацієнта, всі його відвідування і відповідні рецепти.



15

Інструменти для пошуку вразливостей

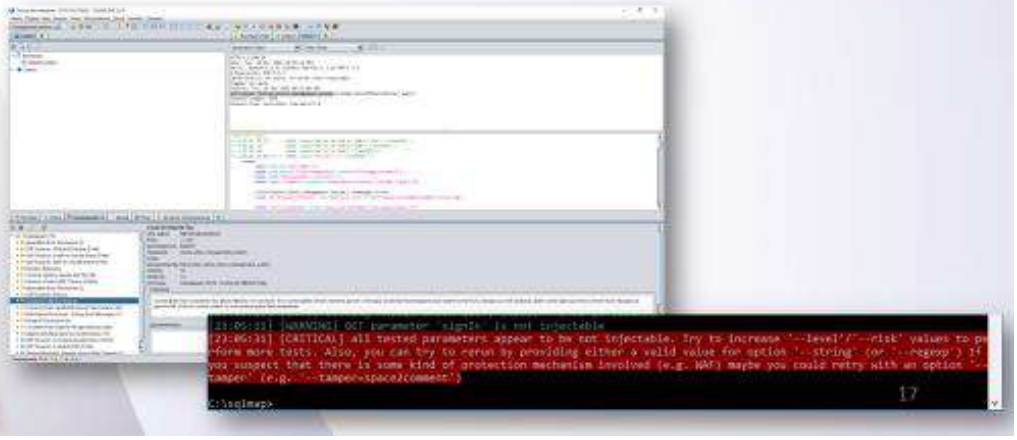
- OWASP ZAP
- W9scan
- Paros
- Tenable.io



Пошук вразливостей

Для тестування веб-додатку було обрано використовувати інструмент від OWASP ZAP.

Для пошуку вразливостей типу SQL ін'єкцій, використовувався інструмент Sqlmap.



17

Результати пошуку

№	Заголовок	Оцінка	Посилання
1	Directory Browsing	2	CWE ID: 548 WASC ID: 48
2	X-Frame-Options Header Not Set	2	CWE ID: 16 WASC ID: 15
3	Absence of Anti-CSRF Tokens	1	CWE ID: 352 WASC ID: 9
4	Cookie No HttpOnly Flag	1	CWE ID: 16 WASC ID: 13
5	X-Content-Type-Options Header Missing	1	CWE ID: 16 WASC ID: 15
6	X-XSS-Protection Off	1	CWE ID: 933 WASC ID: 14

18

Оцінка захищеності

Оцінка рівня загрози вразливостей для веб-застосування:

$$\bar{x} = \frac{\sum k}{n}$$

- k – оцінка рівня загрози кожної вразливості;
- n – кількість знайдених вразливостей в веб-застосуванні.

Оцінка вразливості веб-застосування у відсотках:

$$r = \frac{\bar{x} * 100}{3}$$

Підставивши потрібні значення, отримали такі результати:

- $\bar{x}$ = 1,33;
- r = 44.4%, що відповідає середньому рівню захищеності.

19

Висновки

- Проведено дослідження щодо сучасних проблем безпеки веб-застосувань, описані найпоширеніші і найнебезпечніші вразливості, які актуальні сьогодні, описані методології тестування захищеності веб-додатків і проведено огляд найпопулярніших та найпотужніших інструментів для пошуку вразливостей.
- Протестовано веб-застосування на наявність вразливостей, а також визначена оцінка його захищеності й прописана послідовність дій для її прорахунку.

20