Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Кафедра автоматизації проектування

 енергетичних процесів і систем

**Звіт**

**з циклу лабораторних робіт**

**з дисципліни**

**„Тестування програмного забезпечення на проникнення”**

Лабораторна  робота № 1

Використання Metasploit Framework для визначення вразливостей веб-сайту

Виконала: **Юрченко Богдана**

Студентка групи:   **ТВ-01 мп**

Перевірив викладач: **Сігайов А.О.**

Київ - 2021

Завдання лабораторної роботи :

0. Прочитать перший розділ підручника WEBSECURITY FOR DEVELOPERS.

1. Завантажити та встановити у віртуальну машину дистрибутив Kali Linux: https://www.kali.org/

2. Запустити Metasploit Framework.

3. Запустити утіліту wmap стосовно (бажано свого) веб-сайту та отримати список вразливостей.

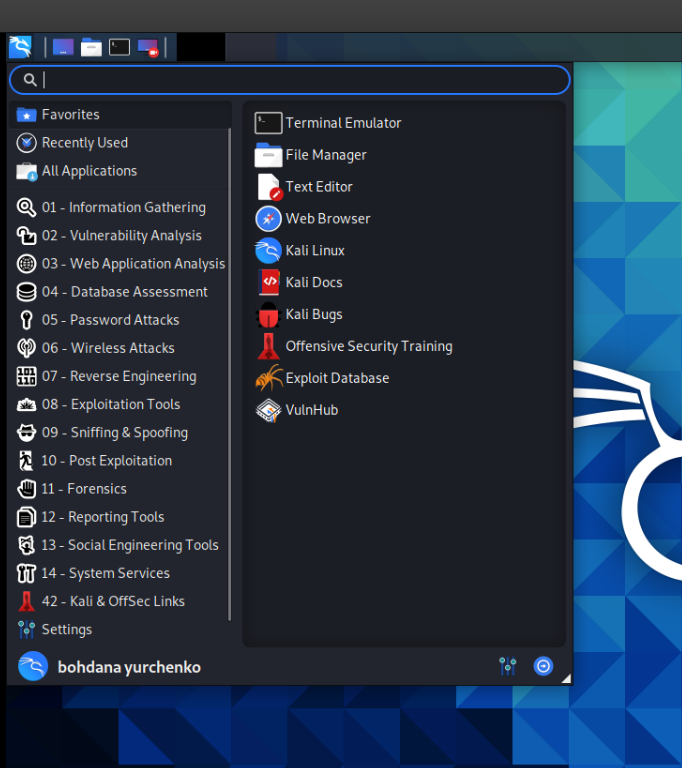
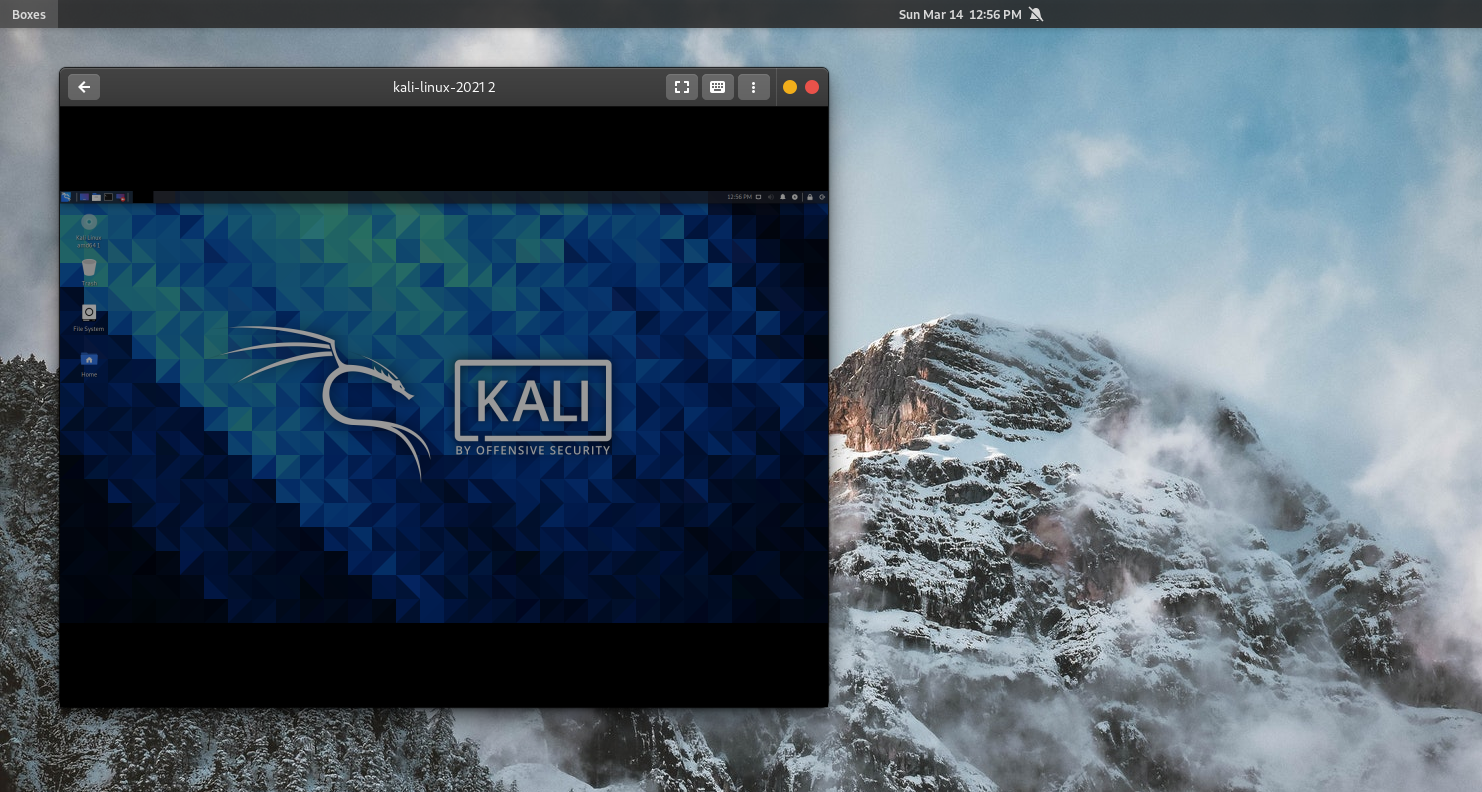
Сайт для сканування у кожного студента повинен бути унікальним, відмінним від тих, що використовуватимуть інші (тому також краще використовувати свій особистий).

Під час роботи було зроблено:

0. Прочитано перший розділ підручника. Де надано інформацію про те, як просто можна отримати доступ до інструментів хакінгу і почати проводити атаки.

В розділі також надається короткий опис утіліти ,використаної в даній роботі.

1. Дистрибутив Лінксу Kali Linux був встановлений на віртуальну машину, створену за допомогою програмного забеспечення Gnome Boxes на Fedora.



На скріншоті показана кількість усіх передвстановлених в дистрибутиві додатків для тестування на проникнення.

2. Запущена утиліта Metasploit Framework.



3. Оскільки в книзі заборонялося використовувати утиліту стосовно “чужих” сайтів (адже це порушення закону), і говорилося, що тестувати можна лише свій власний. А в мене власного сайту немає, сайт був обраний зі списку сайтів, створених спеціально для білого хакінгу, опублікованого за посиланням :

https://securitytrails.com/blog/vulnerable-websites-for-penetration-testing

Був обраний сайт - bWAPP.

bWAPP, або buggy web application, - це преціально розроблений веб-додаток із відкритим кодом. bWAPP створений до проведення успішних проектів тестування на проникнення та етичного злому.

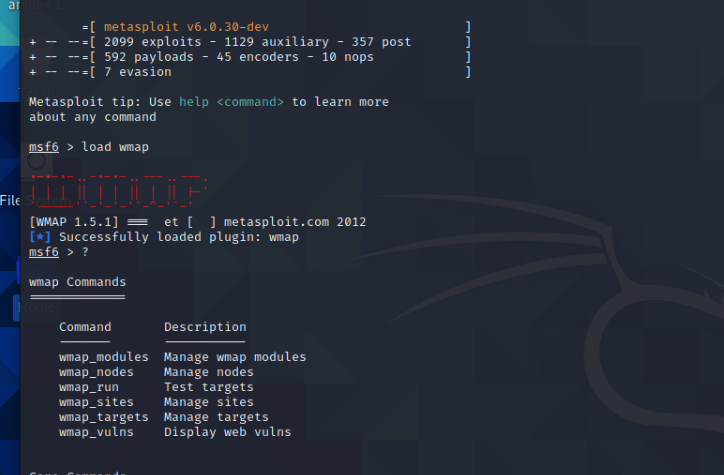
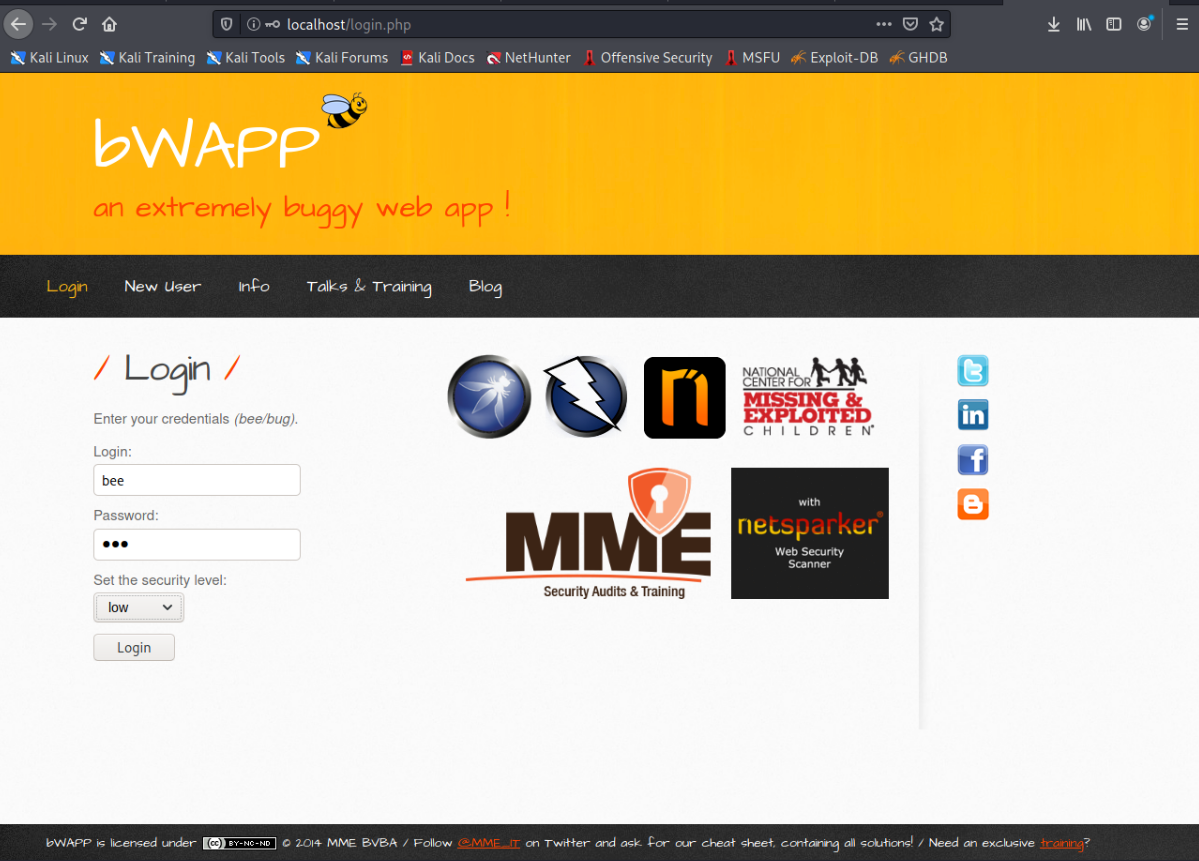
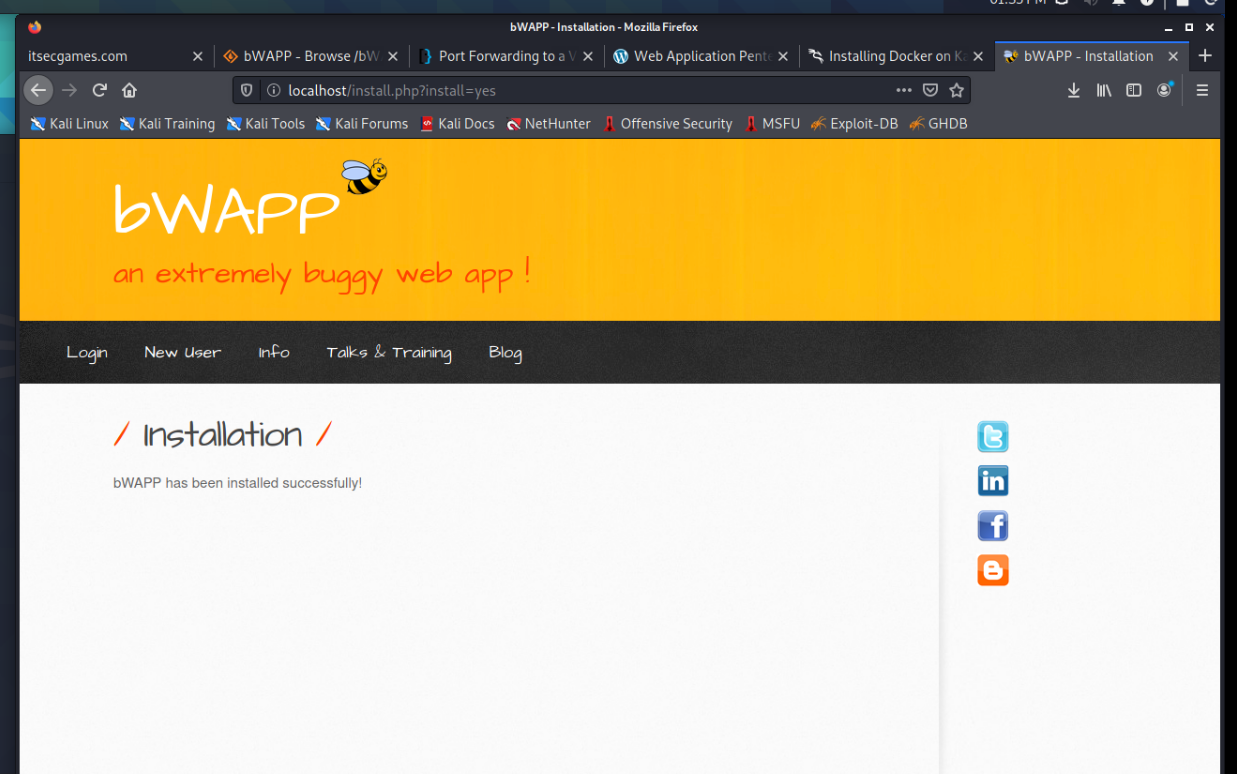
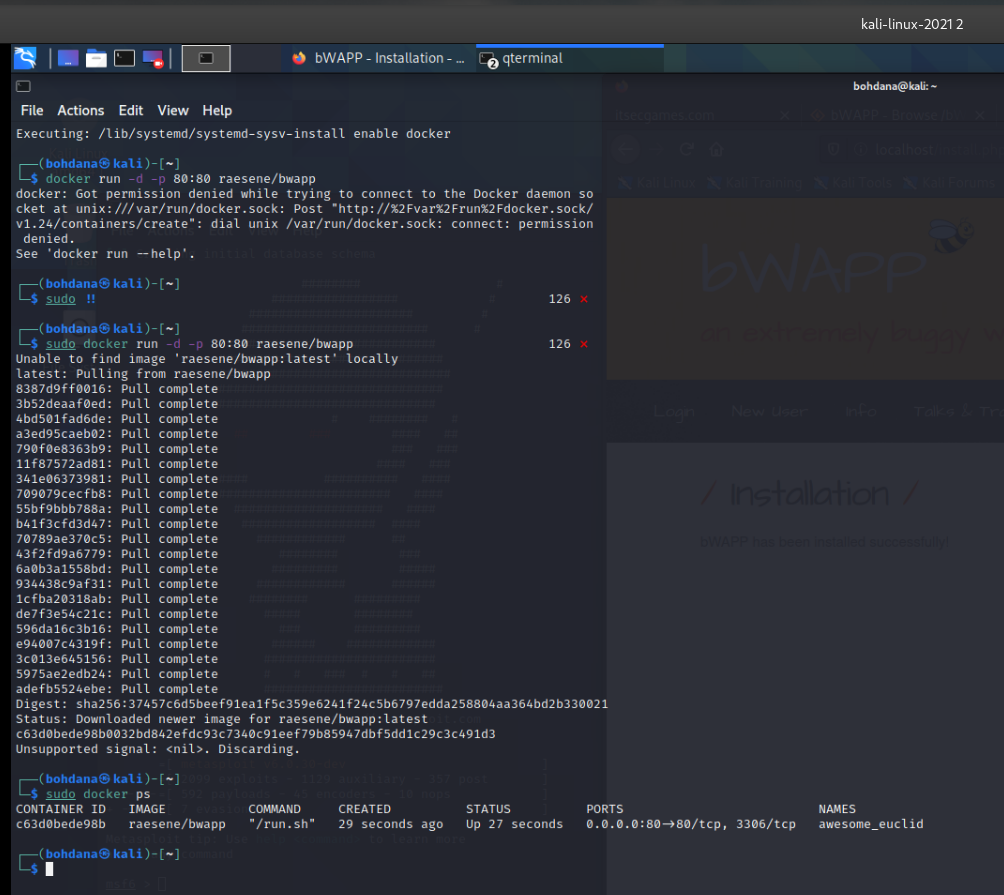
bWAPP має понад 100 веб-вразливостей. Він охоплює всі основні відомі веб-помилки, включаючи всі ризики проекту OWASP Top 10.

Із сайту проекту:

Список із деяких проблем bWAPP:

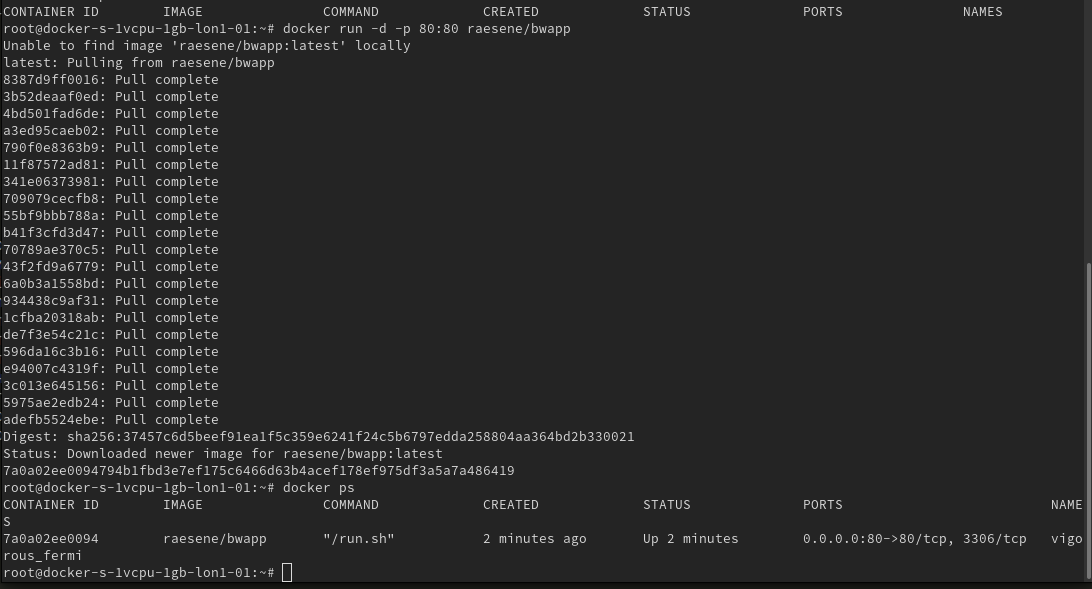
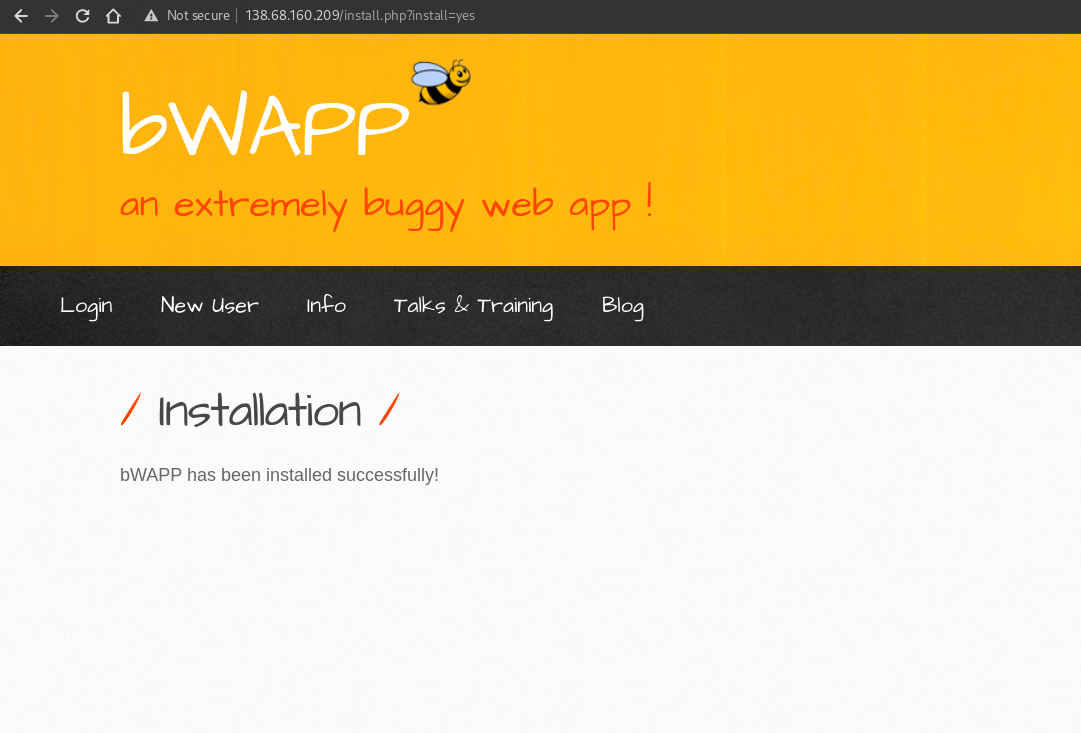
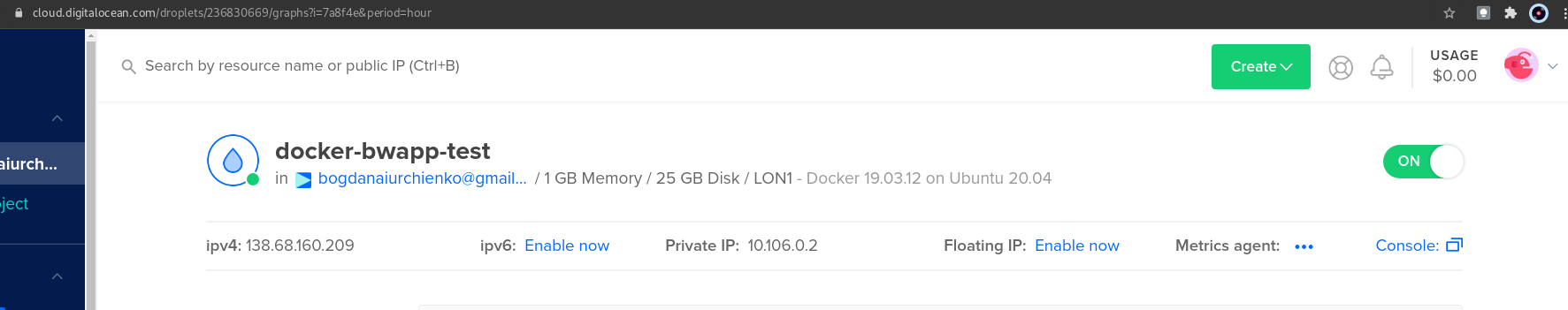
* SQL, HTML, iFrame, SSI, OS Command, XML, XPath, LDAP and SMTP injections
* Blind SQL and Blind OS Command injection
* Bash Shellshock (CGI) and Heartbleed vulnerability (OpenSSL)
* Cross-Site Scripting (XSS) and Cross-Site Tracing (XST)
* Cross-Site Request Forgery (CSRF)
* AJAX and Web Services vulnerabilities (JSON/XML/SOAP/WSDL)
* Malicious, unrestricted file uploads and backdoor files
* Authentication, authorization and session management issues
* Arbitrary file access and directory traversals
* Local and remote file inclusions (LFI/RFI)
* Configuration issues: Man-in-the-Middle, cross-domain policy files, information disclosures,...
* HTTP parameter pollution and HTTP response splitting
* Denial-of-Service (DoS) attacks: Slow HTTP and XML Entity Expansion
* Insecure distcc, FTP, NTP, Samba, SNMP, VNC, WebDAV configurations
* HTML5 ClickJacking, Cross-Origin Resource Sharing (CORS) and web storage issues
* Unvalidated redirects and forwards, and cookie poisoning
* Cookie poisoning and insecure cryptographic storage
* Server Side Request Forgery (SSRF)
* XML External Entity attacks (XXE)

Сайт був встановлений і запущений локально в контейнері за допомогою докер образу.



Виявилося, що дана утиліта не може сканувати локалхост (при спробі додати локалхост в таргет виникає помилка).

Тому для даної лабораторної роботи був створений контейнер із bWAPP на платформі DigitalOcean. Туди і був встановлений сайт для тестування.

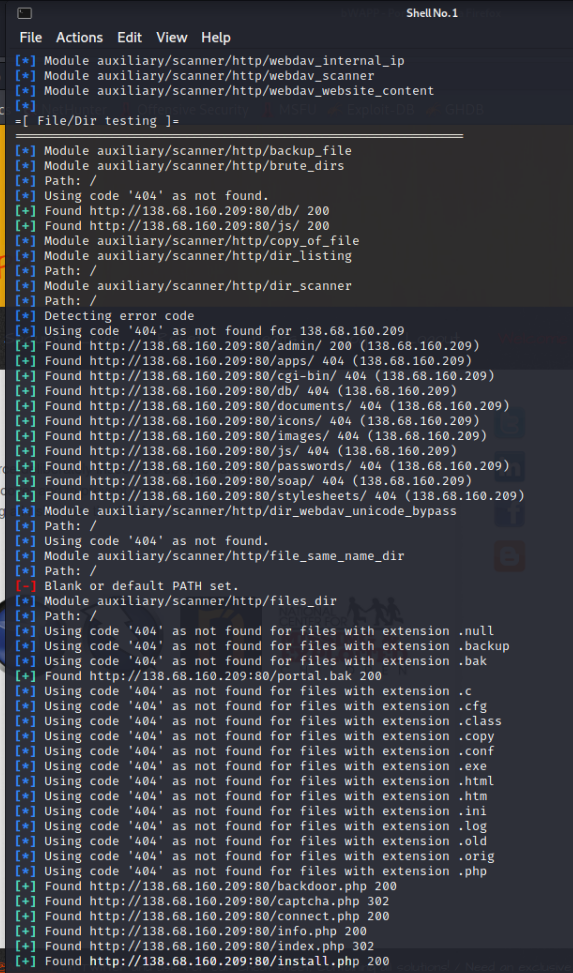
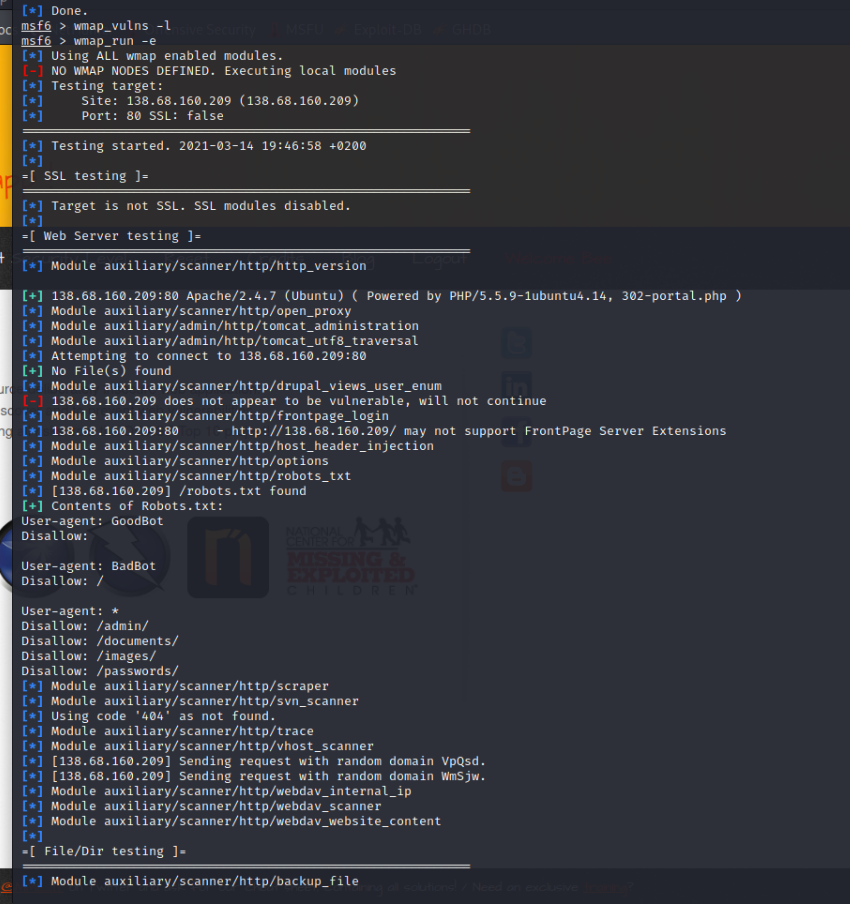
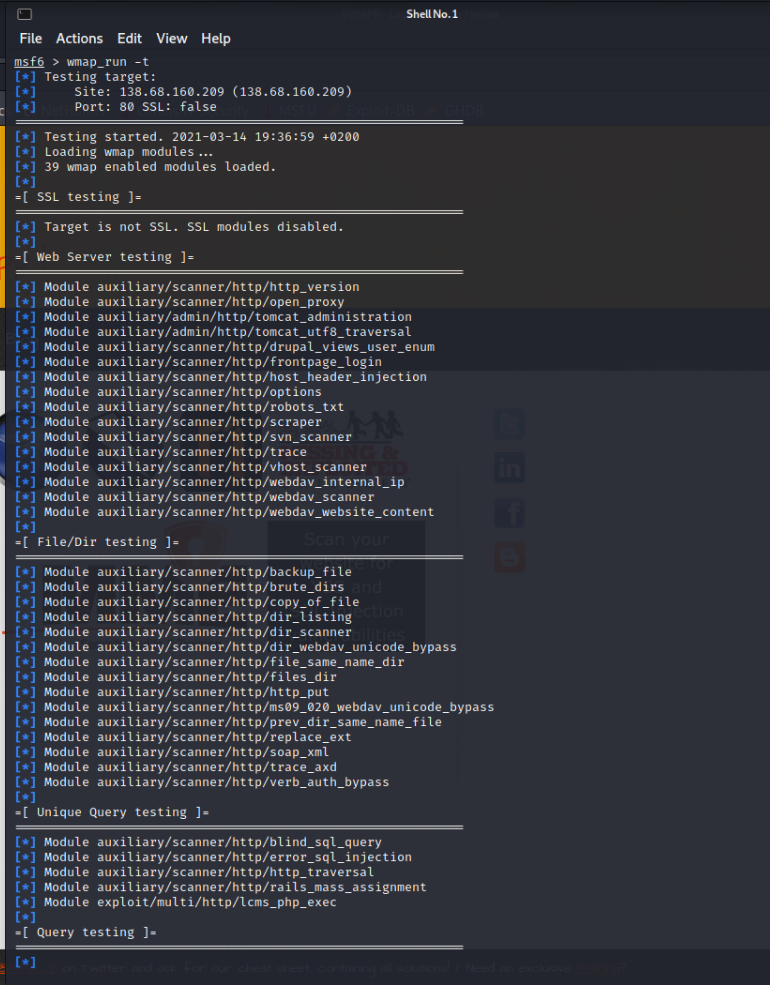


IP сайту для тестування - http://138.68.160.209/login.php

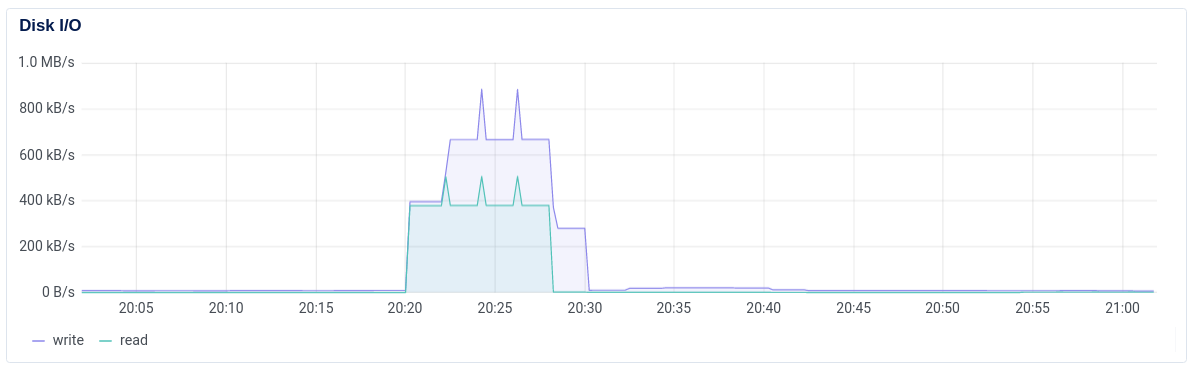
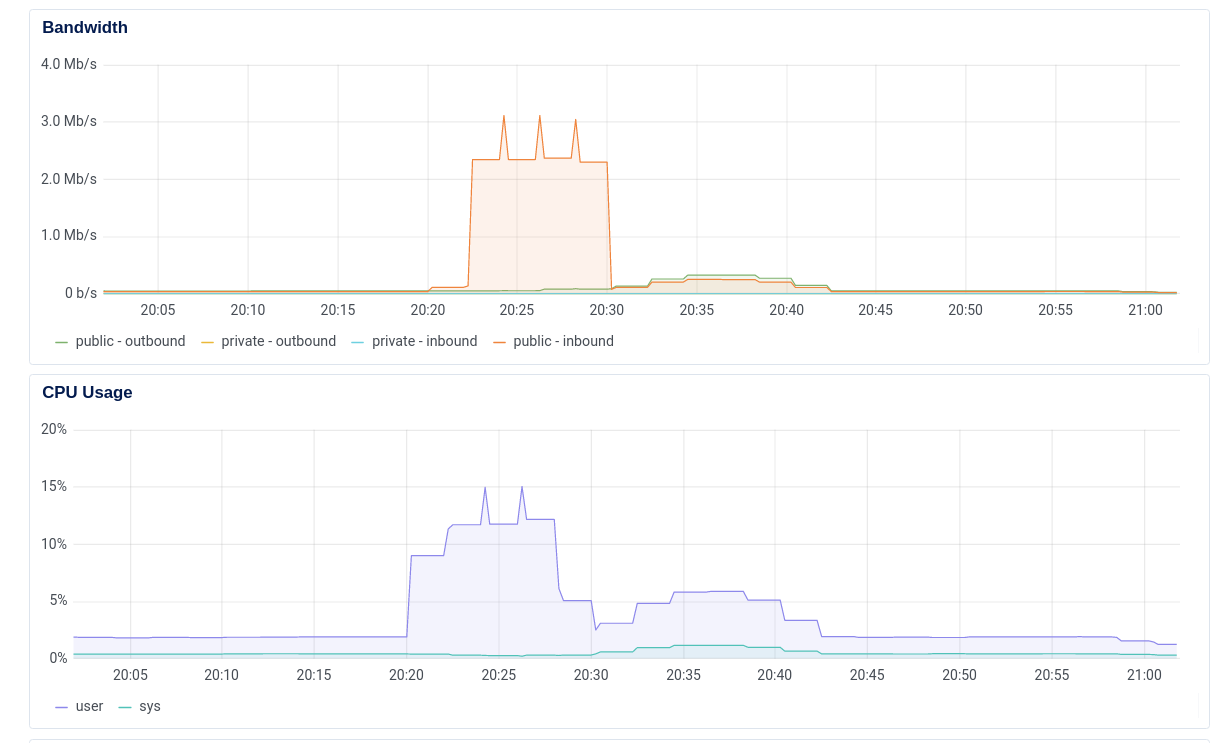
Далі (після налаштування) сайт був доданий в список сайтів і таргетів утиліти :



Після чого можна запускати сканування .



Активність контейнера під час проведення тестування .



Після завершення перевірки можна подивитися список усіх вразливостей за допомогою команди wmap\_vulns -l .

Далі представлено деякі уривки із усього списку вразливостей.

