МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки комп’ютерної та програмної інженерії

Кафедра безпеки інформаційних технологій

**Технології забезпечення конфіденційності і цілісності інформаційних ресурсів**

**Лабораторна робота №4**

Тема: Поняття шкідливого програмного забезпечення. Знайомство з веб-додатком DVWA

Тривалість заняття: 180 хв.

Київ 2023

**Тема:** Поняття шкідливого програмного забезпечення. Знайомство з веб-додатком DVWA

**Мета:** отримати навички роботи з веб-додатком DVWA, та ознайомитись з ним.

**Теоретичні відомості**

**Завдання**

DVWA - це веб-додаток на PHP/MySQL, основна мета якого - стати помічником для професіоналів у сфері безпеки, щоб перевірити свої навички та інструменти у легальному середовищі. Ми постаралися зробити розгортання DVWA максимально простим і створили надбудову, яку можна легко застосувати до балансувальника навантаження EdgeNEXUS ALB-X.

Damn Vulnerable Web Application (DVWA) - це веб-додаток на PHP / MySQL, яке біса вразливе. Його головна мета - допомогти професіоналам з безпеки протестувати їх навички та інструменти в легальному оточенні, допомогти веб-розробникам краще зрозуміти процес безпеки веб-додатків і допомогти і студентам і вчителям у вивченні безпеки веб-додатків в контролюємо оточенні аудиторії.

Мета DVWA попрактикуватися в деяких найпоширеніших веб-вразливості, з різними рівнями складності, з простим прямолінійній інтерфейсом. Зверніть увагу, що є як задокументовані, так і незадокументовані уразливості в цьому програмному забезпеченні. Це зроблено спеціально. Вам пропонується спробувати і виявити так багато вразливостей, як зможете.

Damn Vulnerable Web Application біса вразливе! Не завантажуйте його в публічну html папку вашого хостинг провайдера або на будь-який сервер, який має вихід в Інтернет, оскільки вони будуть скомпрометовані. Рекомендується використовувати віртуальну машину (таку як VirtualBox або VMware), які встановлені в мережевий режим NAT. Усередині гостьовий машини ви можете завантажувати і встановити веб-сервер і бази даних.

Деякі з вразливостей веб-додатків, який містить DVWA;

Брут-форс. Брут-форс HTTP форми сторінки входу; використовується для тестування інструментів по атаці на пароль методом грубої сили і показує небезпечність слабких паролів.

Виконання (впровадження) команд. Виконання команд рівня операційної системи.

Міжсайтовий підробка запиту (CSRF): Дозволяє «атакуючому» змінити пароль адміністратора додатків.

Впровадження (інклуд) файлів. Дозволяє «атакуючому» приєднати вилучені / локальні файли в веб-додаток.

SQL впровадження: Дозволяє «атакуючому» впровадити SQL виразу в HTTP з поля введення, DVWA включає сліпе і засноване на помилку SQL впровадження.

Небезпечна вивантаження файлів. Дозволяє «атакуючому» вивантажити шкідливі файли на веб-сервер.

Міжсайтовий скриптинг (XSS). «Атакуючий» може впровадити свої скрипти в веб-додаток / базу даних. DVWA включає відображену і збережену XSS.

Великодні яйця: розкриття повних шляхів, обхід аутентифікації і деякі інші.

DVWA має три рівні безпеки, вони змінюють рівень безпеки кожного веб-додатки в DVWA.

Неможливий - цей рівень повинен бути безпечним від всіх вразливостей. Він використовується для порівняння уразливого вихідного коду з безпечним вихідним кодом. До DVWA v1.9 цей рівень був відомий як «високий».

Високий - Це розширення середнього рівня складності, з сумішшю складніших або альтернативних поганих практик в спробі убезпечити код. Уразливості не дозволяють такий простір експлуатації як на інших рівнях.

Середній - Цей рівень безпеки призначений головним чином для того, щоб дати користувачеві приклад поганих практик безпеки, де розробник спробував зробити додаток безпечним, але зазнав невдачі. Він також виступає викликом для користувачів, щоб вони удосконалили свої техніки експлуатації.

Низький - Цей рівень безпеки абсолютно вразливий і зовсім не має захисту. Його призначення бути передовим прикладом серед уразливих веб-додатків, прикладом поганих практик програмування і служити платформою навчання базовим технікам експлуатації.

Також в DVWA ви можете включити або відключити PHP-IDS.

PHP-IDS - це популярна PHP система виявлення вторгнень (IDS), які також відомі як фаєрволи веб-додатків (Web Application Firewall (WAF)). PHP-IDS працює за допомогою фільтрації по чорному списку потенційно уразливого коду будь-якого користувача введення. PHP-IDS використовується в DVWA для служіння живим прикладом, як WAF може допомогти поліпшити безпеку в веб-додатках, а в Damn Vulnerable Web Application (DVWA) - випадку, як WAF можна обійти. PHP-IDS може бути включена або відключена одним кліком по відповідній кнопці.

DVWA НЕ емулює уразливості веб-додатків, уразливості всередині DVWA є справжніми і, отже, подбайте як слід про те, де ви збираєтеся встановити DVWA.

DVWA робить активні дії для захисту користувачів де це тільки можливо. Про це говорять впадають в очі написи, в тому числі в самому додатку, з попередженнями. До DVWA можна отримати доступ тільки з localhost, а не з віддаленої машини, це виконана налаштуванням певних правил у файлі .htaccess, який є частиною програми.

DVWA також містить файл robots.txt, якщо додаток все-таки було вивантажено на веб-сервер з Інтернет-доступом, цей файл заборонить пошуковим машинам індексувати додаток.

На кожної сторінки, що містить уразливість, є зовнішні посилання на ресурси, які містять додаткову інформацію, що стосується конкретної уразливості. При кліці на зовнішні посилання, віддалений сервер може збирати таку інформацію як 'Referer' HTTP. Ця інформація містить URL, де встановлено додаток, потенційно, адміністратори сервера можуть переглядати цю інформацію і скомпрометувати сервер, де встановлена ​​DVWA. З цих причин все зовнішні посилання DVWA проходять через довірені проксі третьої сторони, який очищає будь-яку чутливу інформацію з HTTP заголовків.

**Комп'ютерний вірус** ([англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) computer virus) — комп'ютерна програма, яка має здатність до прихованого самопоширення. Одночасно зі створенням власних копій [віруси можуть завдавати шкоди](https://uk.wikipedia.org/wiki/%D0%A8%D0%BA%D1%96%D0%B4%D0%BB%D0%B8%D0%B2%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B8%D0%B9_%D0%B7%D0%B0%D1%81%D1%96%D0%B1): знищувати, пошкоджувати, викрадати дані, знижувати або й зовсім унеможливлювати подальшу працездатність [операційної системи](https://uk.wikipedia.org/wiki/%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) комп'ютера. Розрізняють [файлові](https://uk.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB%D0%BE%D0%B2%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81), [завантажувальні](https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D0%B2%D0%B0%D0%BD%D1%82%D0%B0%D0%B6%D1%83%D0%B2%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81) та [макровіруси](https://uk.wikipedia.org/wiki/%D0%9C%D0%B0%D0%BA%D1%80%D0%BE-%D0%B2%D1%96%D1%80%D1%83%D1%81). Можливі також комбінації цих типів. Нині відомі десятки тисяч комп'ютерних вірусів, які поширюються через мережу Інтернет по всьому світу.

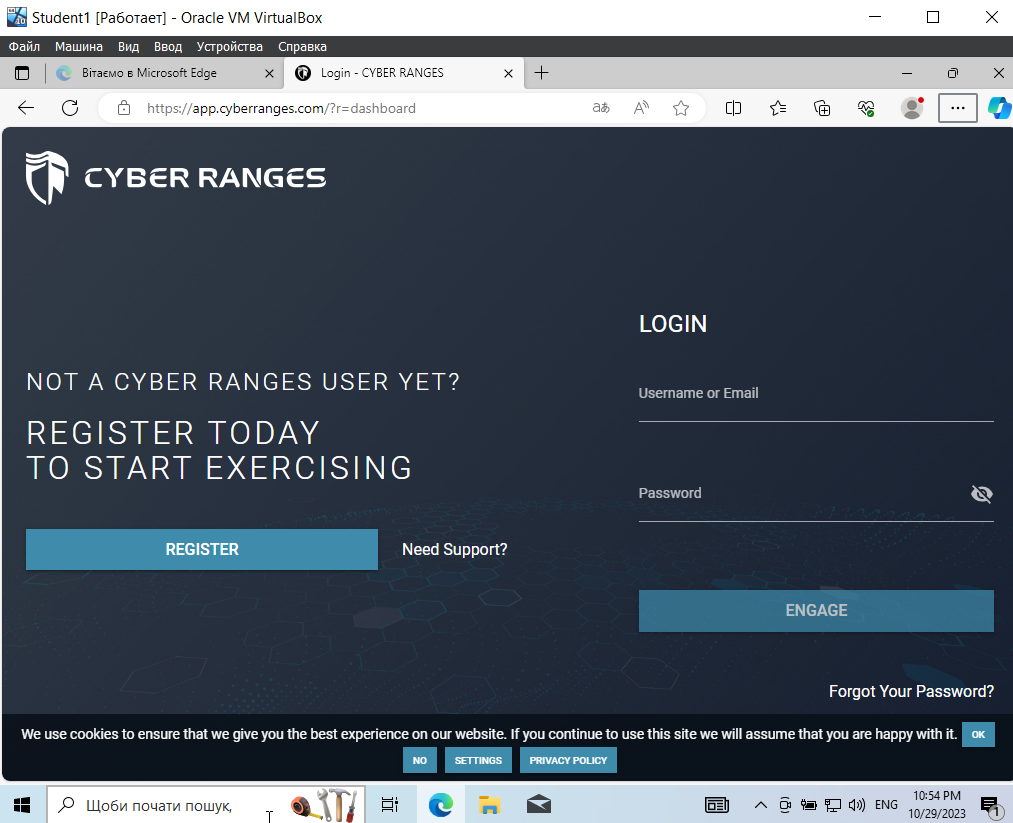
Розробники вірусного програмного забезпечення використовують засоби соціальної інженерії і інформацію про вразливості цільового ПЗ, щоб заражати системи і розповсюджувати вірус. Необізнані користувачі [ПК](https://uk.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80) помилково відносять до комп'ютерних вірусів також інші види [зловмисного ПЗ](https://uk.wikipedia.org/wiki/%D0%97%D0%BB%D0%BE%D0%B2%D0%BC%D0%B8%D1%81%D0%BD%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B8%D0%B9_%D0%B7%D0%B0%D1%81%D1%96%D0%B1) — програми-шпигуни чи навіть [спам](https://uk.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B0%D0%BC).

Щороку комп'ютерні віруси причиняють шкоди розміром в декілька мільярдів доларів, викликаючи системні критичні помилки, зупиняючи великі сайти та вебзастосунки, знищуючи або модифікуючи файли, підвищуючи час відгуку[[1]](https://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%27%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B8%D0%B9_%D0%B2%D1%96%D1%80%D1%83%D1%81#cite_note-1).

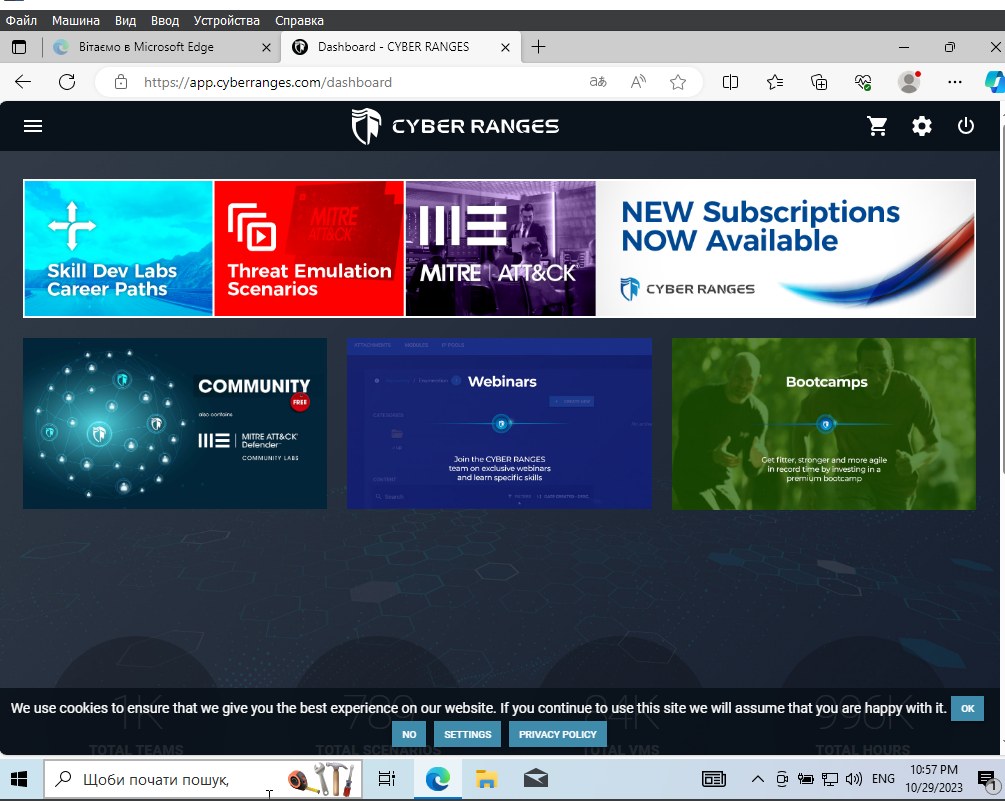
За створення та поширення шкідливих програм (в тому числі вірусів) у багатьох країнах передбачена кримінальна відповідальність. Зокрема, в Україні поширення комп'ютерних вірусів переслідується і карається відповідно до [Кримінального кодексу](https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BC%D1%96%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9_%D0%BA%D0%BE%D0%B4%D0%B5%D0%BA%D1%81_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8) (статті 361, 362, 363). Приклади вірусів: [Neshta](https://uk.wikipedia.org/wiki/Neshta), [Staog](https://uk.wikipedia.org/wiki/Staog), [Archiveus](https://uk.wikipedia.org/wiki/Archiveus).

**Завдання**

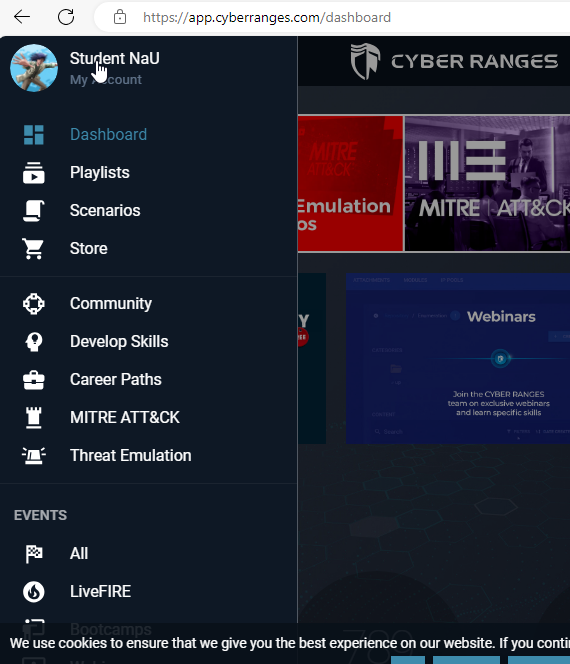
1. Запустіть встановлену на вашому комп’ютері віртуальну машину (вона була створена вами в лабораторній роботі 2, якщо у вас вона відсутня, перейдіть в лабораторну роботу 2, та виконайте пункти 1-19).
2. Запустіть браузер який встановлений на віртуальній машині (Microsoft Edge), та введіть в пошукову строку таке посилання <https://app.cyberranges.com/?r=/dashboard> (копіювання з лабораторної роботи в віртуальну машину не спрацює, потрібно вводити вручну).



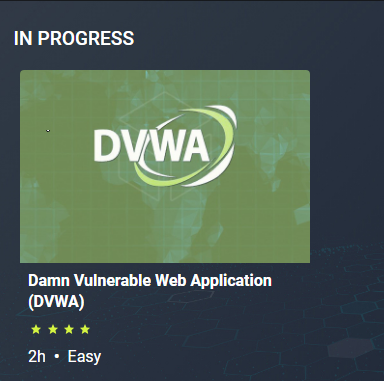
1. На цій сторінці вам потрібно натиснути кнопку register, та слідувати інструкціям з реєстрації. Якщо ви все зробили правильно, то відриється таке вікно.



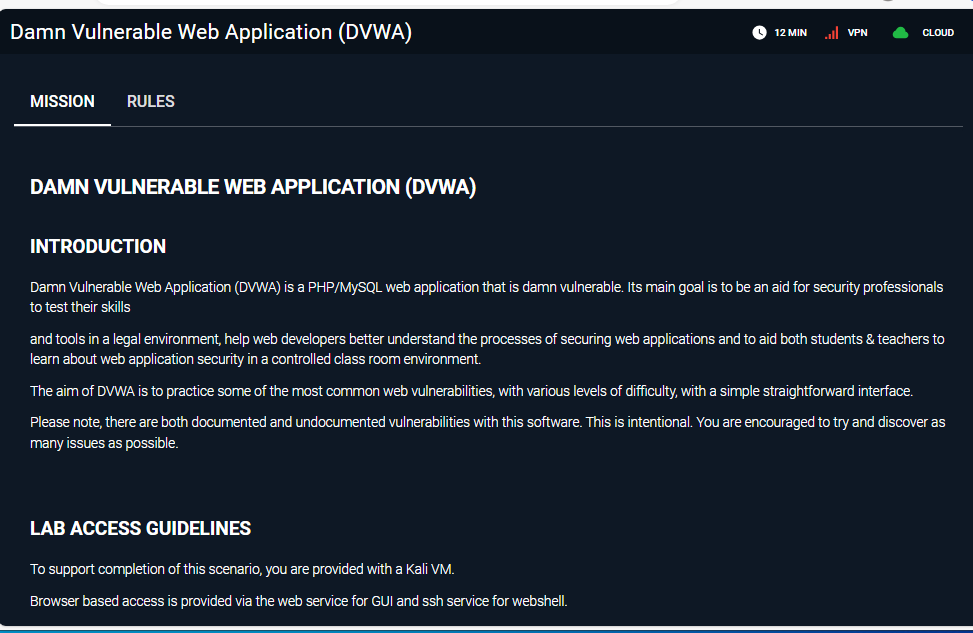
1. Вам потрібно натиснути на три рисочки в лівому верхньому кутку та вибрати Scenarios.



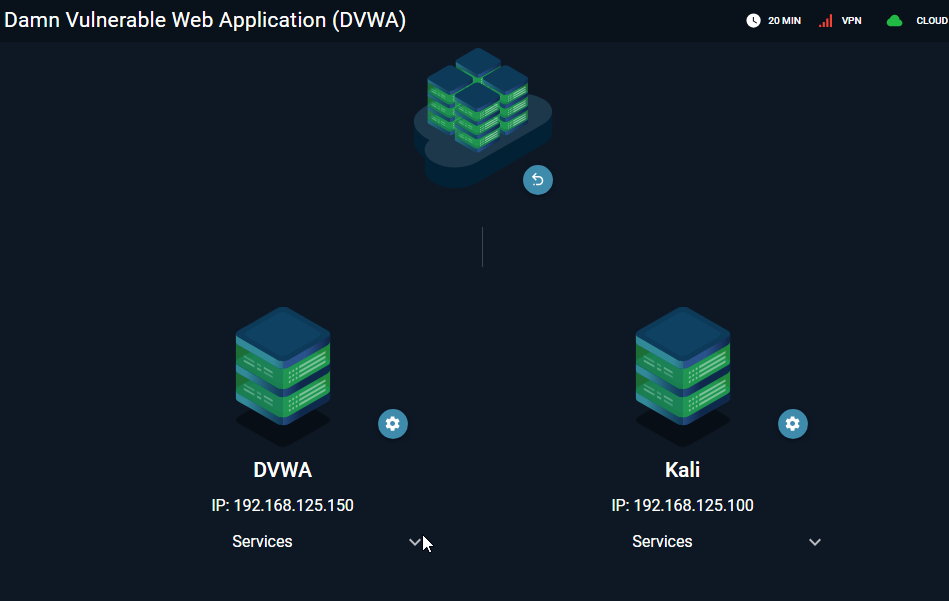
1. На сторінці що відкрилась, вам потрібно знайти цей сценарій, та натиснути на цей сценарій,



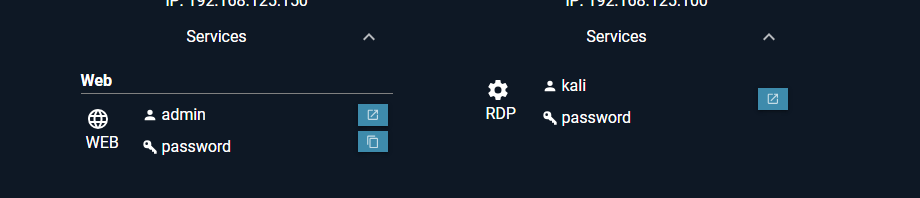
1. Вам потрібно натиснути кнопку start, та дочекатись завершення його завантаження.
2. Перечитайте всі розділи в цьому сценарії (Mission, Rules), якщо ви не знаєте англійської мови, то використовуйте онлайн перекладач, можна навіть онлайн перекладач з телефона, якщо у вас немає онлан перекладача, скачайте його з Appstore або з Google Play.



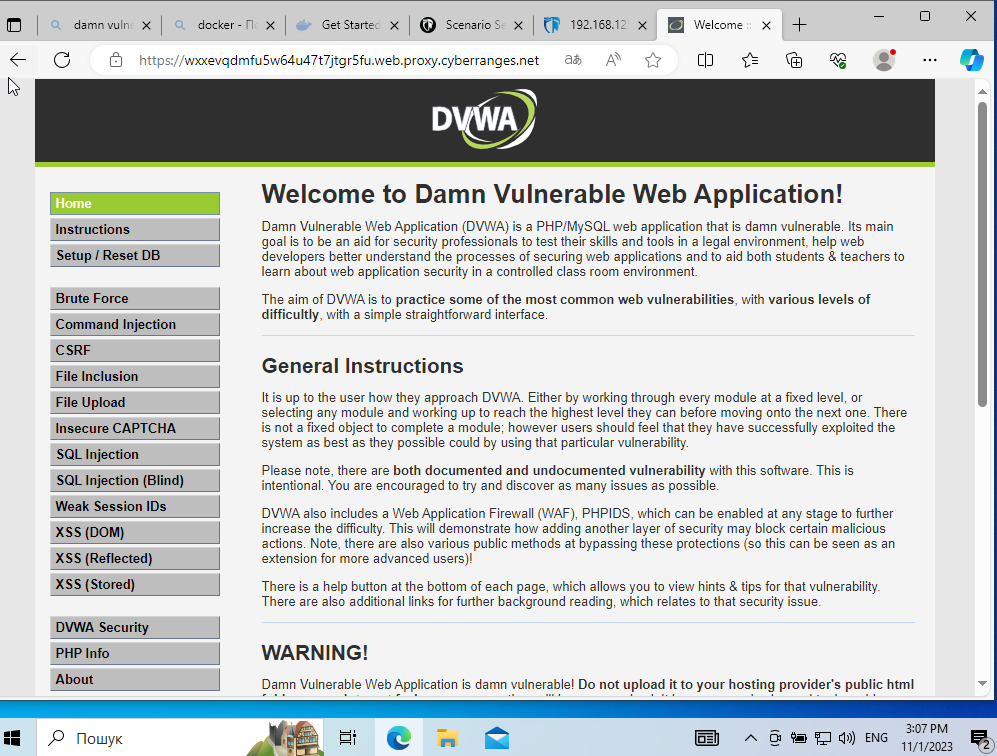
1. Тепер перейдіть на вкладку Servers



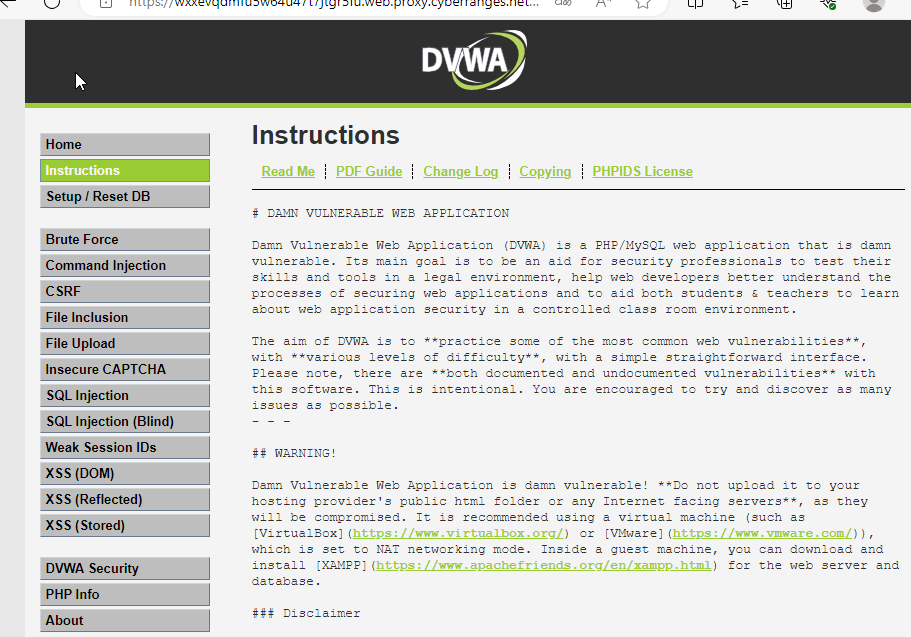
1. Натисніть на стрілочки в низ



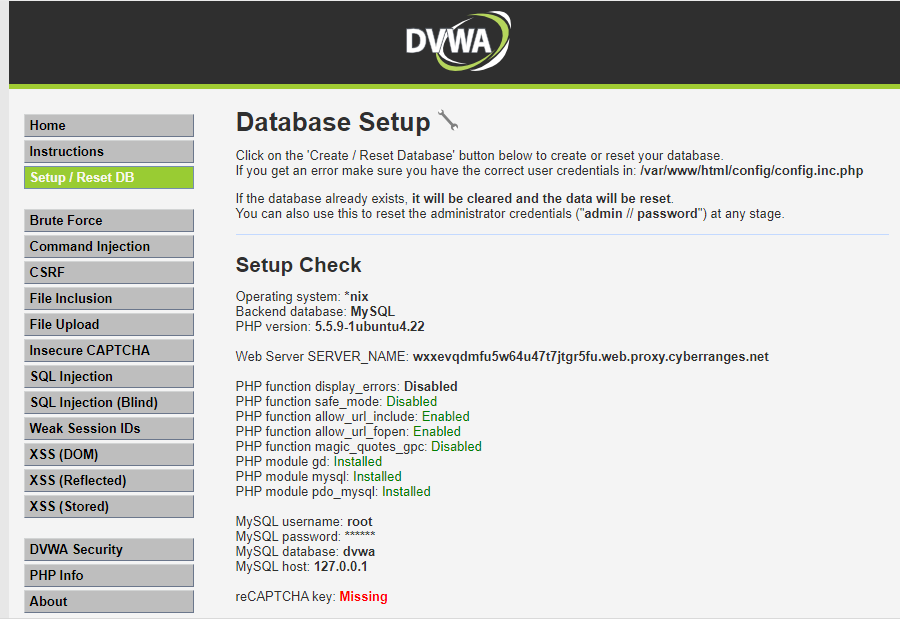
1. Натисніть на кнопку  біля надпису admin та kali.
2. У вікні яке відкрилось, прочитайте всю інформацію на вкладці home. Перейдіть по всім посилання та перегляньте інформацію яка там знаходиться.



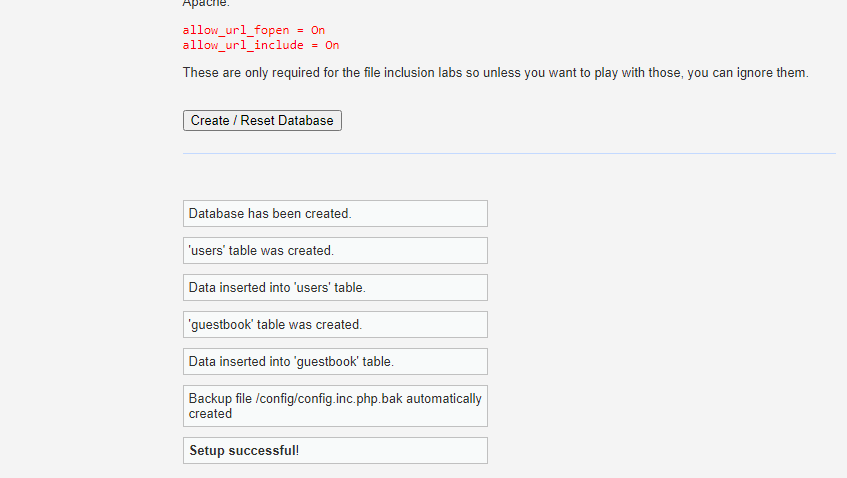
1. Далі перейдіть на вкладу Instructions, прочитайте всю інформацію на цій вкладці. Перейдіть по всім посилання та перегляньте інформацію яка там знаходиться.



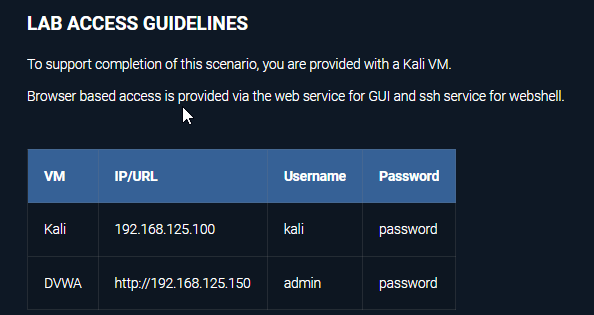
1. Після цього перейдіть на вкладку Setup/Reset DB



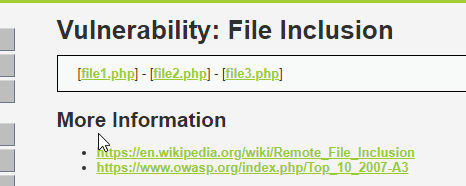
1. На цій же вкладці натисніть кнопку , після чого буде написана наступна інформація як на малюнку



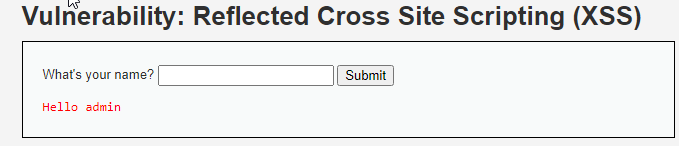
1. Перейдіть на наступну вкладку(Brute Force), як логін введіть: admin, а як пароль: password. Та перегляньте інформацію яка є в More Information.
2. Перейдіть на вкладку Command Injection, та введіть як IP адрессу, адресу машини Kali. Та натисніть кнопку submit. Gерегляньте інформацію яка є в More Information.



1. На вкладці CSRF, введіть поточний пароль(password) та потім його змініть. Та перегляньте інформацію яка є в More Information.
2. На вкладці File Inclusion, перегляньте вміст файлів 1, 2, 3. Та перегляньте інформацію яка є в More Information.



1. На вкладці File Upload перегляньте інформацію яка є в More Information.
2. На наступній вкладці також перегляньте інформацію яка є в More Information.
3. На вкладці SQL Injection та SQL Injection(blind), як User ID – введіть admin. Та перегляньте інформацію яка є в More Information.
4. На наступній вкладці натисніть кнопку Generate.
5. На вкладці XSS(DOM), виберіть мову, та перегляньте інформацію яка є в More Information.
6. На вкладці XSS(Reflected), введіть номер вашої групи поле для ім’я. Та перегляньте інформацію яка є в More Information.



1. На наступній вкладці, введіть в поле ім’я номер вашої групи, а в поле повідомленні, введіть таку фразу «Student nau», натисніть кнопку . Та перегляньте інформацію яка є в More Information.
2. Прочитайте інформацію на всіх вкладках які залишились.
3. Дайте відповідь на контрольні питання, зробіть висновки та занесіть їх до звіту. Звіт має містити скріншоти виконаної вами роботи.

**Контрольні питання**

1. Що таке комп’ютерні віруси?
2. Які бувають комп’ютерні віруси?
3. Опишіть основні види мережевих черв’яків.
4. Які існують способи зараження комп’ютера вірусами?
5. Опишіть основні ознаки зараження комп’ютера вірусами.
6. Поясніть різницю між поняттями вірус та шкідливе програмне забезпечення.
7. Що таке DVWA?