Силабус курсу
БЕЗПЕКА WEB РЕСУРСІВ

Ступінь вищої освіти – бакалавр
Рік навчання: 3
Семестр: 6
Кількість кредитів: 5
Мова викладання: українська

Керівник курсу

ПІП	Тарас Цаволик
Контактна інформація	tth@wunu.edu.ua

Опис дисципліни

Курс **"БЕЗПЕКА WEB РЕСУРСІВ"** знайомить студентів із: основами WEB атак та захисту від них; особливостями використання SQL injection; особливостями використання різних XSS атак; особливостями атаки на заголовки хостів HTTP (HTTP Host Header attacks); отруєння веб-кешом. Ця анотація надає огляд ключових аспектів та мету цього курсу.

Головні аспекти курсу включають наступне:

1. Загрози та Уразливості: Розгляд аспектів, які створюють загрози для веб-ресурсів, такі як крос-сайтовий скриптінг (XSS), крос-сайтовий запрос (XSRF/CSRF), SQL-ін'єкції та інші.
2. Аутентифікація та Авторизація: Розгляд методів забезпечення коректної аутентифікації та авторизації користувачів, включаючи багаторівневий доступ та безпеку паролів.
3. Контроль доступу: Вивчення методів обмеження доступу до конфіденційної інформації та функціональності.
4. Захист сесій: Розгляд методів захисту ідентифікаторів сесій та уникнення сесійної уразливості.
5. Захист від SQL-ін'єкцій: Вивчення та застосування методів для запобігання атакам на базу даних через SQL-ін'єкції.
6. Захист від крос-сайтових атак: Розгляд методів для запобігання крос-сайтовому скриптінгу (XSS) та крос-сайтовим запитам (XSRF/CSRF).
7. Шифрування та HTTPS: Вивчення шифрування даних та застосування HTTPS для забезпечення конфіденційності даних між користувачем та сервером.
8. Середовище безпеки браузера: Розгляд налаштувань безпеки браузера та інструментів розробника для виявлення уразливостей.
9. Захист від DDoS-атак: Вивчення методів виявлення та запобігання атакам з великою кількістю запитів (DDoS).
10. Навчання користувачів: Розгляд важливості навчання користувачів щодо кібербезпеки та соціальної інженерії.
11. Забезпечення внутрішньої безпеки: Розгляд аспектів внутрішньої безпеки, таких як доступ розробників та адміністраторів.
12. Сертифікація та аудит безпеки: Розгляд процесів сертифікації безпеки та аудиту для визначення уразливостей.
13. Сучасні тренди в безпеці: Вивчення останніх трендів та розробка стратегій для протидії новим загрозам.
14. Законодавство та нормативи: Розгляд законодавства та нормативних вимог, які стосуються кібербезпеки в певних галузях.
15. Практичні вправи та випробування: Застосування отриманих знань на практиці через вправи та випробування.

Курс **"Безпека веб-ресурсів"** відіграє важливу роль у захисті веб-сайтів та додатків від загроз та забезпеченні конфіденційності та цілісності даних.

Структура курсу

Години лек/пр	Тема	Результати навчання	Завдання
2/2	Введення в безпеку WEB ресурсів	Вивчення основ WEB безпеки	Поточне опитування
2/2	Міжсайтові сценарії XSS атаки	Як працює XSS. Типи XSS атак. Відбиті XSS сценарії. Збережені XSS сценарії. Тестування виявлених вразливостей	Поточне опитування
2/2	Міжсайтові сценарії XSS на основі DOM атаки	Тестування на виконання JavaScript. DOM XSS у поєднанні з відображеними та збереженими даними	Поточне опитування
2/2	SQL ін'єкції	Впрлив успішних SQL атак. Отримання прихованих даних. Підміна логіки програми. Вивчення баз даних. Запобігання SQL ін’єкцій	Поточне опитування
2/2	SQL-ін'єкційні UNION атаки	Вплив UNION атак. Пошук кількості совбців під час атаки. Використання SQL – ін’єкцій UNION для отримання даних з таблиць баз даних. Сліпі SQL ін’єкції	Поточне опитування
5/5	XML (XXE) ін’єкція	Що таке XML (XXE) ін’єкція? Вразливості XML (XXE). Типи атак XXE. Використання XXE для отримання файлів з веб ресурсів. Сліпі вразливості XXE. XXE атаки через завантаження файлів. Запобігання вразливостей XXE.	Поточне опитування
5/5	Отруєння веб - кешом	Основні поняття отруєння веб – кешом. Вплив атак на отруєння веб - кешом. Запобігання отруєнню веб – кешом.	Поточне опитування
5/5	Атаки заголовку хоста HTTP.	Протокол HTTP. Маршрутизація трафіку через посередника. Вразливості заголовка хоста HTTP. Запобігання атак заголовків хоста.	Поточне опитування
5/5	Вразливості розкриття інформації.	Пошук та використання вразливостей розкриття інформації. Оцінка вразливостей при розкритті інформації. Запобігання вразливостей при розкритті інформації.	Поточне опитування

Рекомендовані джерела інформації

1. Kimminich B. Pwining OWASP Juice Shop. 2020. – 301 p.
2. Andrew Hoffman. Web Application Security. Published by O’Reilly Media, Inc. 2020. – 331 p.

3. Joseph Menn. Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World, June 4, 2021. – 272 p.
4. Christopher Hadnagy. Social Engineering: The Science of Human Hacking, July 31, 2022 – 320p.
5. Kevin Mitnick. The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data, September 10, 2022 - 320 pages.
6. Charles Arthur. Cyber Wars: Hacks that Shocked the Business World 1st Edition, May 29, 2021 - 248 pages
7. Bruce Schneier. Click Here to Kill Everybody: Security and Survival in a Hyper-connected World, October 8, 2022 - 336 pages

Політика оцінювання

Політика щодо дедлайнів та перескладання: Для виконання індивідуальних завдань і проведення контрольних заходів встановлюються конкретні терміни. Перескладання модулів відбувається з дозволу дирекції факультету за наявності поважних причин (наприклад, лікарняний).

Політика щодо академічної доброчесності: Використання друкованих і електронних джерел інформації під час контрольних заходів заборонено.

Політика щодо відвідування: Відвідування занять є обов'язковим компонентом оцінювання. За об'єктивних причин (наприклад, карантин, воєнний стан, хвороба, закордонне стажування) навчання може відбуватись в онлайн формі за погодженням із керівником курсу.

Оцінювання

Модуль 1		Модуль 2		Модуль 3	Модуль 4	Модуль 5
10%	10%	10%	10%	5%	15%	40%
Поточне оцінювання	Модульний контроль 1	Поточне оцінювання	Модульний контроль 2	Тренінги	Самостійна робота	Екзамен
Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №1-5.	Підсумкова письмова робота за темами №1-5.	Оцінка за даний модуль визначається як середнє арифметичне за захист лабораторних робіт №6-7.	Підсумкова письмова робота за темами №6-7.	Визначається як середнє арифметичне з оцінок за виконання та презентацію одного завдання тренінгу.	Визначається як середнє арифметичне за виконання та презентацію одного завдання самостійної роботи.	Теоретичні питання: 2 питання по 30 балів - max 60 балів. Практичне завдання - max 40 балів

Шкала оцінювання:

ECTS	Бали	Зміст
A	90–100	відмінно
B	85–89	добре
C	75-84	добре
D	65-74	задовільно
E	60-64	достатньо
FX	35-59	незадовільно з можливістю повторного складання
F	1-34	незадовільно з обов'язковим повторним курсом