МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

ЗАТВЕРДЖУЮ

Декан ФКІТ
Ігор ЯКИМЕНКО
_____
«___»_____ 2024 р.

ЗАТВЕРДЖУЮ

Проректор з науково-
педагогічної роботи
Віктор ОСТРОВЕРХОВ
_____
«___»_____ 2024 р.

РОБОЧА ПРОГРАМА

з дисципліни «Безпека WEB ресурсів»
ступінь вищої освіти - бакалавр
галузь знань - 12 Інформаційні технології
спеціальність 125 Кібербезпека
освітньо-професійна програма – Кібербезпека

Кафедра кібербезпеки

Форма навчання	Курс	Семестр	Лекції (год.)	Лаб. (год.)	ІРС (год.)	Тренінг (год.)	СРС (год.)	Разом (год.)	іспит (сем.)
денна	3	6	30	30	4	8	78	150	6

Тернопіль –2024

Робоча програма складена на основі освітньо-професійної програми підготовки бакалавра галузі знань 12 Інформаційні технології спеціальності 125 Кібербезпека, затвердженої Вченою радою ЗУНУ (протокол №9 від 15.06.2022 р.).

Робочу програму склав к.т.н., доцент, доцент кафедри кібербезпеки, Тарас ЦАВОЛИК.

Робоча програма затверджена на засіданні кафедри кібербезпеки, протокол № 1 від 26.08.2024 р.

Завідувач кафедри кібербезпеки _____ Василь ЯЦКІВ

Розглянуто та схвалено групою забезпечення спеціальності Кібербезпека та захист інформації, протокол № 1 від 30.08.2024 р.

Голова групи
забезпечення спеціальності _____ Василь ЯЦКІВ

Гарант освітньо-професійної
програми _____ Михайло КАСЯНЧУК

СТРУКТУРА РОБОЧОЇ ПРОГРАМИ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Опис дисципліни «Безпека WEB ресурсів»

Дисципліна - «Безпека WEB ресурсів»	**Галузь знань, спеціальність, СВО**	**Характеристика навчальної дисципліни**
Кількість кредитів – 5	Галузь знань – 12 Інформаційні технології	Статус дисципліни – обов'язкова Мова навчання - українська
Кількість залікових модулів - 5	Спеціальність - 125 Кібербезпека	Рік підготовки: *Денна - 3* Семестр: *Денна - 6*
Кількість змістових модулів – 3	Ступінь вищої освіти – бакалавр	Лекції (год): *Денна - 30* Лабораторні заняття (год): *Денна - 30*
Загальна кількість годин – 150 год.		Самостійна робота (год): *Денна* – 78 Тренінг (год): *Денна* – 8 Індивідуальна робота (год): *Денна – 4*
Тижневих годин: 10 год., з них аудиторних – 4 год.		Вид підсумкового контролю – іспит

2. Мета й завдання вивчення дисципліни «Безпека WEB ресурсів»

2.1. Мета вивчення дисципліни

Програма та тематичний план дисципліни орієнтовані на глибоке та ґрунтовне засвоєння студентами основних понять щодо особливостей безпеки WEB ресурсів.

Ця дисципліна відноситься до дисциплін циклу професійної та практичної підготовки. Метою викладання курсу є надання студентам знань про захист Web–технологій, засвоєння можливостей використання різноманітних атак та протидія їм на WEB ресурси.

Вивчення курсу "Безпека WEB ресурсів" вимагає цілеспрямованої роботи над вивченням спеціальної літератури, активної роботи на лекціях та практичних заняттях, самостійної роботи та виконання індивідуальних завдань.

2.2. Завдання вивчення дисципліни

У результаті вивчення курсу "Безпека WEB ресурсів" студенти повинні засвоїти:

- основи WEB атак та захисту від них;
- особливості використання SQL injection;
- особливості використання різних XSS атак;
- особливості атаки на заголовки хостів HTTP(HTTP Host Header attacks);
- отруєння веб-кешом.

Завдання лекційних занять.

Мета проведення лекцій полягає у тому, щоб ознайомити студентів із основними відомостями щодо атак та захисту WEB ресурсів.

Мета проведення лекцій полягає у:

- викладенні студентам у відповідності з програмою та робочим планом основних понять безпеки WEB ресурсів;
- сформувати у студентів цілісну систему теоретичних знань з курсу "Безпека WEB ресурсів".

Завдання лабораторних занять.

Мета проведення лабораторних занять полягає у тому, щоб виробити у студентів практичні навички атакуючої безпеки WEB ресурсів.

Завдання проведення лабораторних занять:

- ознайомити з особливостями ураження WEB ресурсів;
- ознайомитись з сучасними засобами для виявлення вразливостей WEB ресурсів;
- отримання навиків з захисту WEB ресурсів;
- глибше засвоїти та закріпити теоретичні знання, які були одержані на лекціях.

2.3. Найменування та опис компетентностей, формування котрих забезпечує вивчення дисципліни:

– Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

– Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

2.4. Передумови для вивчення дисципліни

Вивчення курсу «Безпека WEB ресурсів» передбачає наявність систематичних та ґрунтовних знань із суміжних курсів, таких як «Вища математика», «Основи програмування», «Кібернетична безпека», «Комп’ютерні мережі» , «Технології WEB 3.0».

2.5. Результати навчання

– Використовувати сучасне програмно апаратне забезпечення інформаційно комунікаційних технологій.

– Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно правових документів.

– Забезпечувати процеси захисту та функціонування інформаційно телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

– Використовувати програмні та програмно апаратні комплекси захисту інформаційних ресурсів.

– Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах.

– Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

– Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах.

– Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

– Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

– Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

– Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно телекомунікаційних систем.

– Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

– Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

– Використовувати інструментарій для моніторингу процесів в інформаційно телекомунікаційних системах.

3. Програма навчальної дисципліни «Безпека WEB ресурсів»

Змістовий *модуль 1.* Виявлення атак на веб ресурси.

Тема 1. Введення в безпеку WEB ресурсів.

Вивчення основ WEB безпеки.

Література: 1 – 7.

Тема 2. Міжсайтові сценарії XSS атаки.

Як працює XSS. Типи XSS атак. Відбиті XSS сценарії. Збережені XSS сценарії. Тестування виявлених вразливостей.

Література: 1 – 7.

Тема 3. Міжсайтові сценарії XSS на основі DOM атаки.

Тестування на виконання JavaScript. DOM XSS у поєднанні з відображеними та збереженими даними.

Література: 1 – 7.

Тема 4. SQL ін'єкції.

Вплив успішних SQL атак. Отримання прихованих даних. Підміна логіки програми.

Вивчення баз даних. Запобігання SQL ін’єкцій.

Література: 1 – 7.

Тема 5. 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.

Література: 1 – 7.

Змістовий модуль 2. **Атаки та ін’єкції веб ресурсів.**

Тема 6. 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.

Література: 1 – 7.

Тема 7. Отруєння веб - кешом.

Основні поняття отруєння веб – кешом. Вплив атак на отруєння веб - кешом. Запобігання отруєнню веб – кешом.

Література: 1 – 7.

Змістовий модуль 3. Атакаки на заголовки HTTP та викриття вразливостей.

Тема 8. Атаки заголовку хоста HTTP.

Протокол HTTP. Маршрутизація трафіку через посередника. Вразливості заголовка хоста HTTP. Запобігання атак заголовків хоста.

Література: 1 – 7.

Тема 9. Вразливості розкриття інформації.

Пошук та використання вразливостей розкриття інформації. Оцінка вразливостей при розкритті інформації. Запобігання вразливостей при розкритті інформації.

Література: 1 – 7.

4. Структура залікового кредиту з дисципліни «Безпека WEB ресурсів»

	Кількість годин					
	Лек-ції	Лаб. заняття	СРС	ІРС	Тренінг	Контрольні заходи
Змістовий модуль 1. Виявлення атак на веб ресурси						
Тема 1. Введення в безпеку WEB ресурсів	2	2	4	2	4	Поточне опитування
Тема 2. Міжсайтові сценарії XSS атаки	2	2	4			
Тема 3. Міжсайтові сценарії XSS на основі DOM атаки	2	2	10			
Тема 4. SQL ін'єкції	2	2	10			
Тема 5. SQL-ін'єкційні UNION атаки	2	2	10			
Змістовий модуль 2. Атаки та ін’єкції веб ресурсів						
Тема 6. XML (XXE) ін’єкція	5	5	10	1	2	Поточне опитування
Тема 7. Отруєння веб - кешом	5	5	10			
Змістовий модуль 3. Атаки на заголовки HTTP та викриття вразливостей						
Тема 8. Атаки заголовку хоста HTTP.	5	5	10	1	2	Поточне опитування

Тема 9. Вразливості розкриття інформації	5	5	10			
Разом	30	30	78	4	8	

5. Тематика лабораторних занять

Лабораторне заняття № 1
Тема: XSS атака у контексті HTML.
Мета: Освоїти основи XSS атаки.
Література: 1-7.
Лабораторне заняття № 2
Тема: XSS атака на основі DOM.
Мета: Навчитись виявляти атаки на основі DOM.
Література: 1-7.
Лабораторне заняття № 3
Тема: SQL – ін’єкція.
Мета: Навчитись виконувати SQL – ін’єкції.
Література: 1-7.
Лабораторне заняття № 4
Тема: Union SQL – ін’єкція.
Мета: Навчитись виконувати Union SQL – ін’єкції.
Література: 1-7.
Лабораторне заняття № 5
Тема: XML (XXE) ін’єкції.
Мета: Навчитись проводити XXE атаки.
Література: 1-7.
Лабораторне заняття № 6
Тема: Отруєння веб - кешем.
Мета: Навчитись працювати та виявляти ін’єкції веб - кешем.
Література: 1-7.
Лабораторне заняття № 7
Тема: HTTP атаки.
Мета: Навчитись проводити HTTP атаки.
Література: 1-7.

6. Самостійна робота студентів

Самостійна робота студентів є однією з обов’язкових складових частин модулю залікового кредиту з курсу «Безпека WEB ресурсів». Виконується у вигляді теоретичних доповідей кожним студентом самостійно на основі одного сформованого завдання, що охоплює основні теми курсу.

Пропонована тематика завдань:

1 Основні відомості про кібербезпеку
2 Пасивний збір інформації
3 Активний збір інформації про мережу
4 Механізми захисту мережі від збору інформації, сканування та проникнення
5 Застосування криптографічних сервісів
6 Аналіз трафіку в комп’ютерних мережах
7 Перехоплення сесій передачі даних в комп’ютерних мережах
8 Безпека в безпровідних мережах
9 Безпека в операційних системах
10 Шкідливе програмне забезпечення
11 Переповнення буферу

12 Безпека веб-серверів та веб-застосувань
13 Атака «відмова в обслуговуванні»
14 SQL-ін’єкції
15 Соціальна інженерія
16 Тестування на вразливість до атак

7. Організація та проведення тренінгу з дисципліни Безпеки WEB ресурсів

Порядок проведення тренінгу:

1. Вступна частина проводиться з метою ознайомлення студентів з темою тренінгу.

2. Організаційна частина полягає у створенні робочого настрою у колективі студентів.

3.Практична частина реалізується шляхом виконання одного завдання з певних проблемних питань теми тренінгу.

4. Підведення підсумків. Обговорення результатів виконаних завдань. Обмін думками з питань, що виносяться на тренінг.

Тематика тренінгу: Проектування предметної області та написання WEB програми для її реалізації.

Мета тренінгу: забезпечення студентів комплексними теоретичними знаннями та практичними навичками.

Завдання тренінгу: презентувати результати виконання роботи.

№ п/п	Вид роботи	Порядок проведення тренінгу
1	Огляд та аналіз	Здійснити аналіз та види WEB атак.
2	Підходи	Розглянути підходи до запобігання атак на WEB ресурси.
3	Результат програмного забезпечення	Представити результати реалізації у вигляді готового програмного web-орієнтованого рішення

8. Засоби оцінювання та методи демонстрування результатів навчання

У процесі вивчення дисципліни «Безпека WEB ресурсів» використовуються наступні методи оцінювання навчальної роботи студента:

– поточне опитування;
– підсумкове тестування за кожним змістовним модулем;
– оцінювання виконання лабораторних робіт;
– самостійна робота студента;
– підсумковий письмовий іспит.

9. Критерії, форми поточного та підсумкового контролю

Підсумковий бал (за 100 – бальною шкалою) з дисципліни «Безпека WEB ресурсів» визначається як середньозважена величина, в залежності від питомої ваги кожної складової залікового кредиту %:

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	Теоретичні питання: 2 питання по 30 балів - max 60 балів. Практичне завдання -

					завдання самостійної роботи.	max 40 балів

Шкала оцінювання:

За шкалою ТНЕУ	За національною шкалою	За шкалою ECTS
90-100	відмінно	**A** (відмінно)
85-89	добре	**B** (дуже добре)
75-84		**C** (добре)
65-74	задовільно	**D** (задовільно)
60-64		**E** (достатньо)
35-59	незадовільно	**FX** (незадовільно з можливістю повторного складання)
1-34		**F** (незадовільно з обов'язковим повторним курсом)

11. Інструменти, обладнання та програмне забезпечення, використання яких передбачає навчальна дисципліна

№	Найменування	Номер теми
1	Мультимедійний проектор та проєкційний екран	1 -9
2	Персональні комп'ютери	1 -9
3	Комунікаційне програмне забезпечення (Zoom) для проведення занять у режимі он-лайн (за необхідності)	1 -9
4	Комунікаційна навчальна платформа (Moodle) для організації дистанційного навчання (за необхідності)	1 -9
5	Наявність доступу до мережі Інтернет	1 -9

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