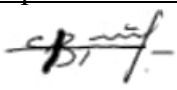
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Львівський національний університет імені Івана Франка
Факультет прикладної математики та інформатики
Кафедра кібербезпеки

Затверджено
На засіданні кафедри кібербезпеки
факультету прикладної математики та інформатики
Львівського національного університету імені Івана Франка
(Протокол № 15/23 від 29 серпня 2023 р.)



Завідувач кафедри ____ П.С.Венгерський

Силабус з навчальної дисципліни "Веб проектування, розробка та безпека додатків", що викладається в межах ОПП Кібербезпека першого (бакалаврського) рівня вищої освіти для здобувачів з спеціальності 125 – кібербезпека та захист інформації

Львів 2023 р.

Назва дисципліни	**Веб проектування, розробка та безпека додатків**
Адреса викладання дисципліни	Львівський національний університет імені Івана Франка, вул. Університетська 1, м. Львів, Україна, 79000
Факультет та кафедра, за якою закріплена дисципліна	Факультет прикладної математики та інформатики Кафедра кібербезпеки
Галузь знань, шифр та назва спеціальності	12 – інформаційні технології 125 – кібербезпека та захист інформації
Викладачі дисципліни	Беляєв Ігор Сергійович, асистент кафедри кібербезпеки (лекції та лабораторні заняття)
Контактна інформація викладачів	Igor.Beliaiev@lnu.edu.ua https://ami.lnu.edu.ua/en/employee/i-s-beliaiev Головний корпус ЛНУ ім. І. Франка, каб. 380. м. Львів, вул. Університетська, 1
Консультації з питань навчання по дисципліні відбуваються	Консультації проводять раз на тиждень згідно з оприлюдненим розкладом консультацій викладача. Можливі онлайн консультації через Zoom чи Microsoft Teams. Для погодження часу онлайн консультацій слід писати на електронну пошту викладача.
Сторінка курсу	https://ami.lnu.edu.ua/course/
Інформація про дисципліну	Дисципліна “ Інструменти проведення тестування на проникнення” є вибірковою дисципліною з спеціальності 125 – кібербезпека та захист інформації для освітньої програми Кібербезпека, яка викладається у 7-му семестрі в обсязі 6-х кредитів (за Європейською Кредитно-Трансферною Системою ECTS).
Коротка анотація дисципліни	Дисципліна призначена для формування у студентів високої кваліфікації в області безпечного програмування. Його метою є надання учасникам комплексних знань та практичних навичок щодо захисту програмного забезпечення від різноманітних вразливостей, що можуть виникати протягом усього життєвого циклу програми. Курс охоплює різні аспекти безпечного програмування, включаючи основні принципи проектування та розробки безпечного коду, методи уникнення вразливостей, використання технологій тестування програмного забезпечення та впровадження заходів захисту. Особлива увага приділяється відомим стандартам безпеки програмного забезпечення, таким як OWASP, щоб студенти могли працювати відповідно до найвищих стандартів безпеки.
Мета та цілі дисципліни	Мета курсу полягає у підготовці студентів до практичного застосування знань і навичок у галузі безпечного програмування. Через акцент на практичних завданнях та вправах, студенти здобудуть необхідний досвід у виявленні та усуненні вразливостей у програмному забезпеченні.
Література для вивчення дисципліни	1. Wilson G.DevSecOps: A leader’s guide to producing secure software without compromising flow, feedback and continuous improvement, 2020. – 278 p. 2. Janca T. Alice and Bob Learn Application Security, 2020. – 288 p. 3. Kohnfelder K. Designing Secure Software, 2021. – 312 p. 4. Raje G. Security and Microservice Architecture on AWS: Architecting and Implementing a Secured, Scalable Solution 1st Edition, 2021. – 394 p. 5. Blokdyk G. Secure Coding Best Practices A Complete Guide – 2021. – 309 p.

Обсяг курсу	Загальний обсяг: 180 годин. Аудиторних занять: 64 год., з них 32 год. лекцій та 32 год. лабораторних робіт. Самостійної роботи: 116 год.
Очікувані результати навчання	У результаті вивчення навчальної дисципліни студент має набути таких компетентностей: **знати:** • Основні безпекові практики OWASP; • Основні методи уникнення вразливостей; • Типові моделі атак; • Тестування на вразливості; • Методи захисту даних користувача; • Вимоги до безпеки програмного забезпечення; • Концепції статичного та динамічного аналізу коду; • Засоби автоматизованого тестування; • Типові помилки програмування та методи їх усунення; • Основні принципи проектування безпечного коду; • Безпечна обробка помилок та безпечне логування; • Рекомендації щодо запобігання вразливостям. **вміти:** • Розробляти веб-додатки з використанням сучасних технологій інтернет-розробки. • Розуміти основні принципи та методи проектування інтерфейсу користувача для веб-додатків. • Знати техніки та інструменти для забезпечення безпеки веб-додатків, включаючи виявлення та усунення вразливостей. • Вміти працювати з базами даних для зберігання та обробки інформації у веб-додатках. • Розробляти ефективні механізми аутентифікації та авторизації користувачів у веб-додатках. • Знати процес тестування веб-додатків та вміти виконувати тестування на вразливості для забезпечення їхньої безпеки. **Курс забезпечує набуття таких компетентностей: КЗ 1, КЗ 2, КЗ 3, КЗ 4, КЗ 5, КЗ 7, КФ 1, КФ 5, КФ 7, КФ 9, КФ 10; та програмних результатів навчання: ПРН 1, ПРН 2, ПРН 3, ПРН 4, ПРН 5, ПРН 6, ПРН 7, ПРН 8, ПРН 9, ПРН 16, ПРН 22, ПРН 27, ПРН 31, ПРН 33, ПРН 34, ПРН 36, ПРН 37, ПРН 38, ПРН 40, ПРН 44, ПРН 45, ПРН 46, ПРН 47, ПРН 48.**
Ключові слова	Веб-проектування, розробка веб-додатків, безпека програмного забезпечення, інтерфейс користувача, веб-технології, бази даних, аутентифікація, авторизація, тестування безпеки, вразливості, інтернет-розробка, техніки безпеки.
Формат курсу	Очний Проведення лекцій, лабораторних робіт і консультацій.
Теми	Теми курсу подано в схемі нижче.
Підсумковий контроль, форма	Залік у кінці семестру.
Пререквізити	Для вивчення курсу студенти потребують базові знання з таких дисциплін: 1) Основи кібербезпеки; 2) Операційні системи та комп'ютерні мережі; 3) Тестування на проникнення
Навчальні методи та техніки, які будуть використовуватися	Презентації, лекції Демонстрація інструментів тестування на проникнення Робота з інструментами для тестування на проникнення Індивідуальні завдання

під час викладання курсу	
Необхідне обладнання	Комп'ютер, чи ноутбук з можливістю віртуалізації; Програмне забезпечення віртуалізації: VirtualBox, або VMware; Операційні системи: Windows, Ubuntu, Kali Linux; Програмне забезпечення Burp Suite, або OWASP ZAP;
Критерії оцінювання (окремо для кожного виду навчальної діяльності)	Оцінювання проводиться за 100-бальною шкалою. Бали нараховуються за наступним співвідношенням: • модульний контроль, тестування, усне опитування: 50% семестрової оцінки; максимальна кількість балів 50 • індивідуальні завдання: 50% семестрової оцінки; максимальна кількість балів 50 Підсумкова максимальна кількість балів 100. **Академічна доброчесність**: Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів становлять, але не обмежують, приклади можливої академічної недоброчесності. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її незарахування викладачем, незалежно від масштабів плагіату чи обману. **Відвідання занять** є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції та практичні зайняття курсу. Студенти повинні інформувати викладача про неможливість відвідати заняття. У будь-якому випадку студенти зобов'язані дотримуватися термінів визначених для виконання всіх видів письмових робіт та індивідуальних завдань, передбачених курсом. **Література.** Уся література, яку студенти не зможуть знайти самостійно, буде надана викладачем виключно в освітніх цілях без права її передачі третім особам. Студенти заохочуються до використання також й іншої літератури та джерел, яких немає серед рекомендованих. **Політика виставлення балів.** Враховуються бали набрані при поточному тестуванні, самостійній роботі та бали підсумкового тестування. При цьому обов'язково враховуються присутність на заняттях та активність студента під час практичного заняття; недопустимість пропусків та запізнень на заняття; користування мобільним телефоном, планшетом чи іншими мобільними пристроями під час заняття в цілях не пов'язаних з навчанням; списування та плагіат; несвоєчасне виконання поставленого завдання і т. ін. Жодні форми порушення академічної доброчесності не толеруються.
Питання до контролю	1. Що таке SQL ін'єкція, і як вона може бути використана для атаки на веб-додатки? 2. Які існують види аутентифікації веб-додатків, і які є недоліки кожного з них? 3. Як виявити та усунути вразливості Cross-Site Scripting (XSS)? 4. Що таке міжсайтова подделка запиту (CSRF), і як її можна запобігти? 5. Як забезпечити безпеку паролів користувачів у веб-додатках? 6. Які існують методи захисту від атак міжсайтового сценарію (XSS)? 7. Як забезпечити безпеку сесійних ключів у веб-додатках? 8. Як виявляти та захищати веб-додатки від атак на відмову в обслуговуванні (DoS)? 9. Що таке ін'єкція команд та як її уникнути у веб-додатках? 10. Як забезпечити безпеку перегляду файлів у веб-додатках? 11. Які існують загрози безпеці при роботі з формами у веб-додатках? 12. Які основні методи шифрування використовуються для забезпечення безпеки даних у веб-додатках? 13. Які є переваги та недоліки використання HTTPS у веб-додатках?

	14. Як здійснюється захист від атак на витік інформації через SQL запити? 15. Які існують стратегії валідації та фільтрації введених даних у веб-додатках? 16. Що таке криптографічний солоджувач, і як він використовується для забезпечення безпеки паролів? 17. Як забезпечити безпеку автоматизованих тестів у веб-додатках? 18. Що таке керування сесіями, і як воно впливає на безпеку веб-додатків? 19. Як виявляти та захищати веб-додатки від атак міжсайтової подделки запиту (CSRF)? 20. Які методи захисту від атак на переповнення буфера використовуються у веб-додатках? 21. Як забезпечити безпеку статичних та динамічних скриптів у веб-додатках? 22. Які існують методи захисту від атак на витік інформації через недостатність доступу до даних? 23. Як виявити та усунути вразливості, пов'язані з недостатньою валідацією введених даних? 24. Які є основні принципи захисту від атак на веб-сервери? 25. Що таке захищений HTTP заголовок, і як він використовується для забезпечення безпеки веб-додатків? 26. Як забезпечити безпеку введених даних через веб-форми у веб-додатках? 27. Які існують стратегії моніторингу та реагування на інциденти безпеки у веб-додатках? 28. Як забезпечити безпеку перегляду та завантаження файлів у веб-додатках? 29. Як виявити та захистити веб-додатки від атак на відмову в обслуговуванні (DoS) та атак на затримки? 30. Як здійснюється захист від атак на перехоплення сесій у веб-додатках?
Опитування	Анкету-оцінку з метою оцінювання якості курсу буде надано по завершенню курсу.

Схема курсу:

Тиж.	**Тема, план, короткі тези**	**Форма діяльності (заняття)**	**Література**	**Завдання, год**	**Термін виконання**
1-2	РОЗДІЛ 1. ОСНОВИ БЕЗПЕКИ ВЕБ-ДОДАТКІВ Загрози та вразливості веб-додатків. Принципи проектування безпечних веб-додатків. Техніки виявлення та усунення вразливостей.	лекція, лаб, самостійна робота		4 4 10	2 тижні
3-4	РОЗДІЛ 2. АУТЕНТИФІКАЦІЯ ТА АВТОРИЗАЦІЯ	лекція, лаб, самостійна робо-		4 4 12	2 тижні

	Різновиди методів аутентифікації. Застосування ролей та дозволів у системі авторизації. Захист від атак на автентифікацію та авторизацію.	та			
5-6	РОЗДІЛ 3. БЕЗПЕКА БАЗ ДАНИХ Загрози безпеці баз даних. Методи захисту даних в базах даних. Розгляд технологій шифрування та контролю доступу.	лекція, лаб самостійна робота		4 4 12	2 тижнів
7-8	РОЗДІЛ 4. Тестування безпеки веб-додатків Виявлення та експлуатація вразливостей. Методи тестування на проникнення. Створення безпечних тестових сценаріїв.	лекція, лаб самостійна робота		4 4 12	2 тижні
9-10	РОЗДІЛ 5. Захист від атак Відомі види атак на веб-додатки. Стратегії протидії атакам. Моніторинг та реагування на інциденти безпеки.	лекція, лаб самостійна робота		4 4 10	2 тижні
11-13	РОЗДІЛ 6. Основи криптографії та шифрування Основні концепції криптографії. Застосування шифрування в безпеці веб-додатків. Розгляд відкритих та симетричних алгоритмів шифрування.	лекція, лаб, самостійна робота		6 6 14	3 тижні
14-16	РОЗДІЛ 7. Безпека клієнтської сторони Загрози безпеці клієнтської сторони. Захист від атак на клієнтські дані. Оцінка безпеки веб-браузерів та їх розширень.	лекція, лаб, самостійна робота		6 6 16	3 тижні

				32/32/86	