ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

ТЕХНОЛОГІЇ БЕЗПЕКИ WEB-РЕСУРСІВ / WEB RESOURCE SECURITY TECHNOLOGIES

СИЛАБУС/
SILABUS

ЗАТВЕРДЖЕНО
засіданням кафедри
(протокол №. 1
від «07» серпня 2024 р.)
завідувач кафедри
_____Олена КРИВОРУЧКО

Київ 2024

Назва освітньої компоненти	**ТЕХНОЛОГІЇ БЕЗПЕКИ WEB-РЕСУРСІВ / WEB RESOURCE SECURITY TECHNOLOGIES**
Спеціальність	125 «Кібербезпека та захист інформації»
Освітній ступінь	Другий (магістерський)
Освітньо-професійна програма	**БЕЗПЕКА СИСТЕМ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ В ЕКОНОМІЦІ**
	Лектор: **Лахно Валерій** -професор кафедри інженерії програмного забезпечення та кібербезпеки -доктор технічних наук -професор Резюме викладача: https://nubip.edu.ua/node/37856 е-пошта: **v.lakhno@knute.edu.ua** **lva964@nubip.edu.ua**
	Лектор: **Котенко Наталія** -доцент кафедри інженерії програмного забезпечення та кібербезпеки -кандидат педагогічних наук -доцент Резюме викладача: https://knute.edu.ua/blog/read/?pid=39712&uk Науковий профіль: https://knute.edu.ua/blog/read/?pid=46719 е-пошта: kotenkono@knute.edu.ua
Консультації	https://knute.edu.ua/blog/read/?pid=47103&uk
Програма освітньої компоненти	https://knute.edu.ua/blog/read/?pid=48216
ЗМІСТ ОСВІТНЬОЇ КОМПОНЕНТИ	
Тема 1. Введення в безпеку WEB ресурсів	Історія вебсервісів та їх зв'язок із безпекою. Безпека вебсервісів. Вимоги до безпечного вебзастосунку. Стек стандартів безпечної вебслужби. Нормативна база щодо забезпечення захисту Web-ресурсів. Міжнародні та державні стандарти по забезпеченню безпеки Web-ресурсів. Загальні ризики з якими стикаються вебсервіси. Конфіденційність і цілісність обміну послугами. Основи конфігурації безпеки Інтернету: протокол передачі гіпертексту; HTTPS (протокол передачі гіпертексту через захищені сокети); протокол SSL

	(Secure Sockets Layer); симетричне та асиметричне шифрування; використання протоколу простого доступу до об’єктів (SOAP); протокол SMTP (Simple Mail Transfer Protocol); протокол поштового відділення (POP3); протокол доступу до Інтернету (IMAP). Вебвзлом: вразливості вебсерверів, вебзастосунків і методи злому паролів на основі вебсайтів. Як працюють вебсервери? Типи вразливостей вебсерверів. Вразливості вебзастосунків. Вебтехнології злому паролів. Огляд технологій вебавтентифікації. Брандмауери вебдодатків.
Тема 2. Проєкт по забезпеченню безпеки вебзастосунків	Що таке Open Web Application Security Project (OWASP)? Декілька проєктів над якими працює OWASP: OWASP Security Knowledge Framework (SKF), OWASP Mobile Security Testing Guide (MSTG), OWASP Web Security Testing Guide (WSTG), OWASP Zed Attack Proxy (ZAP). Огляд топ-10 списку OWASP (OWASP TOP 10 2017 / 2021): Injection / Ін'єкція; Broken Authentication / Порушена автентифікація; Sensitive Data Exposure / Незахищеність конфіденційних даних; XML External Entities (XXE) / Зовнішні організації XML (XXE); Broken Access Control / Порушений контроль доступу; Security Misconfigurations / Неправильна конфігурація безпеки; Cross-Site Scripting (XSS) / Міжсайтові сценарії (XSS); Insecure Deserialization / Небезпечна десеріалізація; Using Components with Known Vulnerabilities / Використання компонентів із відомими вразливими місцями; Insufficient Logging and Monitoring / Недостатня реєстрація та моніторинг. Принципи тестування, методологія тестування за OWASP. Активне та пасивне тестування. Розвідка і уразливості вебзастосунків: відкриття вебсторінки / структури програми; збір інформації в вебзастосунках; сканування вразливостей вебзастосунків.
Тема 3. Безпека серверної частини вебзастосунків: SQL-ін'єкція	Що таке ін'єкція SQL (SQLi)? Вплив успішної атака SQL-ін’єкції на конфіденційні дані. Приклади ін'єкції SQL: широкий спектр вразливостей, атак і методів ін'єкції SQL, які виникають у різних ситуаціях. Отримання прихованих даних. Порушення логіки програми. Перевірка бази даних під час атак із застосуванням SQL. Запит типу та версії бази даних. SQL-ін'єкція UNION атаки. Визначення кількості стовпців, необхідних для атаки UNION із впровадженням SQL. «Сліпа» ін’єкція SQL. Використання сліпої ін'єкції SQL шляхом ініціювання умовних відповідей. Як запобігти сліпим атакам SQL-ін'єкції? Виявлення вразливостей ін'єкції SQL. Автоматизація виявлення SQLi. Інструменти для автоматичного пошуку

	SQLi. Ін'єкція SQL другого порядку. Запобігання ін'єкції SQL.
Тема 4. Безпека серверної частини вебзастосунків: автентифікація та авторизація вебзастосунків	Вразливості автентифікації. Різниця між аутентифікацією та авторизацією. Вплив уразливостей аутентифікації на обліковий запис користувача. Вразливості під час входу за паролем. Атаки грубої сили. Брутфорсування імен користувачів. Підбір паролів. Перерахування Username користувача. Блокування облікового запису. Вразливості в багатофакторній аутентифікації. Обхід двофакторної аутентифікації. Перебір кодів підтвердження 2FA. Зберігання користувачів у системі. Скидання паролів користувачів. Відправка паролів електронною поштою. Скидання паролів за допомогою URL-адреси. Зміна паролів користувачів. Запобігання атак на власні механізми аутентифікації. Вразливості авторизації (контролю доступу). Вертикальний контроль доступу. Горизонтальний контроль доступу. Приклади зламаних засобів контролю доступу. Незахищені функції адміністратора. Методи контролю доступу на основі параметрів. Порушений контроль доступу через неправильну конфігурацію платформи. Небезпечні прямі посилання на об’єкт (IDOR). Як запобігти вразливості авторизації (контролю доступу).
Тема 5. Безпека серверної частини вебзастосунків: вразливість SSRF	Безпека серверної частини вебдодатків: введення в server-side-уразливості - SSRF (server-side request forgery). Вплив атак SSRF. Поширені атаки SSRF. Атаки SSRF на інші внутрішні системи. SSRF з вхідними фільтрами на основі чорного списку. SSRF з фільтрами введення на основі білого списку. Обхід фільтрів SSRF через відкриту вразливість переспрямування. «Сліпі» вразливості SSRF. Пошук прихованої поверхні атаки на вразливості SSRF.
Тема 6. Безпека серверної частини вебзастосунків: XXE- ін'єкція	XXE-ін'єкція (ін’єкція зовнішньої сутності XML). Як виникають вразливості XXE. Типи атак XXE. Ін’єкційна атака XXE, яка витягує довільний файл із файлової системи сервера. Використання XXE для виконання атак SSRF. Використання сліпого XXE для ексфільтрації даних поза діапазоном. Використання сліпого XXE для отримання даних через повідомлення про помилки. Використання XXE для отримання даних шляхом перепрофілювання локального DTD.
Тема 7. Безпека клієнтської частини веб-додатків: вразливість XSS	Міжсайтові сценарії (XSS). Як працює XSS. Які існують типи атак XSS. Reflected XSS. Stored XSS. DOM-based XSS (міжсайтові сценарії на основі DOM). Для чого можна використовувати XSS? Вплив вразливостей XSS. Як знайти та перевірити уразливості XSS. Політика безпеки вмісту (CSP).

	Як запобігти XSS -атакам.
Тема 8. Безпека клієнтської частини веб-додатків: атаки CSRF	Підробка міжсайтових запитів (CSRF). Які наслідки атаки CSRF. Як працює CSRF? Як побудувати атаку CSRF. Запобігання атак CSRF. Поширені вразливості CSRF. Перевірка токена CSRF в залежності від методу. Перевірка токена CSRF в залежності від наявності токена. Захист від CSRF на основі рекомендацій. Перевірка Referer залежить від наявності заголовка.
Тема 9. Безпека клієнтської частини веб-додатків: вразливості на основі DOM	Об'єктна модель документа (DOM). Taint-flow vulnerabilities. Огляд поширених вразливостей на основі DOM. Міжсайтові сценарії на основі DOM. Як перевірити міжсайтові сценарії на основі DOM. Як запобігти уразливості DOM-XSS. Що таке відкрите перенаправлення на основі DOM. Маніпулювання файлами cookie на основі DOM. Як запобігти вразливості маніпуляції файлами cookie на основі DOM. Впровадження SQL на стороні клієнта на основі DOM. Який вплив на клієнта SQL-ін'єкція на основі DOM? Який вплив ін'єкції XPath на основі DOM? Який вплив атаки JSON-ін'єкції на основі DOM? Відмова в обслуговуванні на основі DOM.
Тема 10. Безпека клієнтської частини веб-додатків: Clickjacking	Що таке clickjacking (виправлення інтерфейсу користувача). Як побудувати базову атаку clickjacking. Clickjacking з попередньо заповненою формою введення. Поєднання clickjacking з атакою DOM XSS. Багатокроковий clickjacking. Як запобігти clickjacking -атакам. Опції X-Frame. Політика безпеки вмісту (CSP). Захист від clickjacking за допомогою CSP.
Тема 11. Автоматизовані інструменти для аналізу захищеності Web-ресурсів	Сканери безпеки Web-ресурсів: застосунки, фреймворки та онлайн-сервіси. Основні підходи та принципи роботи. Перевірка застосунків на вразливість автоматизованими засобами. Розшифрування звітів про перевірені сайти. Аналіз та рекомендації щодо виправлень зауважень.

СПИСОК ОСНОВНИХ РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Бурячок В.Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В.Л.Бурячок, А.О.Аносов, В.В.Семко, В.Ю.Соколов, П.М.Складанний. –К.:КУБГ, 2019. – 218с.
2. 2. Anoop Singhal, Theodore Winograd, Karen Scarfone. Guide to secure web services. National Institute of Standards and Technology Special Publication 800-95, 2007. - 128 Pages
3. 3. Elie Saad, Rick Mitchell. Owasp Testing Guide v4. Open Web Application Security Project, 2015. - 453 Pages
4. 4. Andrew Homan. Web Application Security Exploitation and Countermeasures for Modern Web Applications. United States of America, 2020. – 331 Pages. ISBN: 978-1-492-08796-0
5. 5. Justin Clarke. SQL Injection Attacks and Defense. Syngress Publishing, Inc., Elsevier, Inc., 2009 - 494 Pages. ISBN 13: 978-1-59749-424-3

РЕЗУЛЬТАТИ ВИВЧЕННЯ ОСВІТНЬОЇ КОМПОНЕНТИ Дисципліна забезпечує оволодіння здобувачами вищої освіти загальними та фаховими компетентностями і досягнення ними програмних результатів навчання:	
КЗ-1	Здатність застосовувати знання у практичних ситуаціях
КЗ-2	Здатність проводити дослідження на відповідному рівні
КЗ-4	Здатність оцінювати та забезпечувати якість виконуваних робіт
КФ1	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки
КФ2	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ5	Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ6	Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ7	Здатність досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому
КФ12	*Здатність виконувати обов'язки внутрішнього консультанта і радника у своїй експертній області.*
КФ13	*Здатність проводити дослідно-експериментальну роботу щодо процедури сканування вразливостей та їх розпізнавання в системах безпеки.*
РН4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач

	професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН10	Забезпечувати безперервність бізнес / операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
РН11	Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
РН12	Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
РН15	Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16	Приймати обґрунтовані рішення з організаційно- технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
РН19	Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
РН22	Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
РН23	Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
РН- 25	*Виконувати обов'язки внутрішнього консультанта/ радника в технічній сфері та галузі авторського права щодо електронних носіїв інформації.*
РН- 27	*Проводити сканування систем безпеки інформаційних ресурсів на вразливості.*
РН- 28	*Застосовувати принципи забезпечення безпеки інформації – збереження конфіденційності, цілісності та доступності.*

ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ ОСВІТИ			
Сума балів, накопичених здобувачем вищої освіти за виконання всіх видів поточних навчальних завдань (робіт) на лабораторних/практичних заняттях, свідчить про ступінь оволодіння ним програмою освітньої компоненти на конкретному етапі її вивчення. Протягом семестру здобувачі освіти можуть набрати від 0 до 100 балів, що переводяться у національну шкалу оцінювання і відповідно у шкалу ЄКТС. Кількість балів відповідає певному рівню засвоєння дисципліни			
Довідник з розподілу оцінок ДТЕУ (Шкала ЄКТС):			
Бали ДТЕУ	Відсоток балів відносно загальної кількості одержаних прохідних балів	Кумулятивний відсоток отриманих прохідних балів	
90-100	20	20	
82-89	10	30	
75-81	20	50	
69-74	10	60	
60-68	40	100	
Роподіл балів за видами робіт:			
Вид роботи	**Бали**	**Вид роботи**	**Бали**
Лабораторна робота 1	**10**	Самостійна робота 1	**2**
Лабораторна робота 2	**10**	Самостійна робота 2	**2**
Лабораторна робота 3	**5**	Самостійна робота 3	**2**
Лабораторна робота 4	**5**	Самостійна робота 4	**2**
Лабораторна робота 5	**5**	Самостійна робота 5	**2**
Лабораторна робота 6	**5**	Самостійна робота 6	**2**
Лабораторна робота 7	**5**	Самостійна робота 7	**2**
		Самостійна робота 8	**2**
		Самостійна робота 9	**2**
		Самостійна робота 10	**2**
		Самостійна робота 11	**2**
Додаткові бали + Захист проєкту	**23**	Наукова робота	**10**
Вимоги до критеріїв оцінювання самостійної роботи студента (оцінювання одного завдання у відсотковому еквіваленті)			
40%	Детальний розгляд сутності та вмісту основних джерел. Подання фактів, ідей і результатів досліджень у логічній послідовності. Правильно проаналізовано поточний стан дослідження проблеми та зроблено огляд перспектив подальшого розвитку даного питання.		
40%	Обґрунтованість аргументів, підтвердження особистого		

	ставлення, пропозиції стосовно вирішення завдання, встановлення напрямків аналізу.
20%	Оформлення звіту у відповідності вимог
Критерії оцінювання самостійної роботи студента (оцінювання одного завдання у відсотковому еквіваленті)	
100%	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
80%	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань
60%	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
40%	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та лабораторних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
20%	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.
0%	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.
ОСНОВНІ ПОЛОЖЕННЯ, ЩО РЕГЛАМЕНТУЮТЬ ОСВІТНІЙ ПРОЦЕС	
діючі положення	https://knute.edu.ua/blog/read/?pid=44402
нормативно-правова база організації освітнього процесу	https://knute.edu.ua/blog/read/?pid=7330&uk

студенту	https://knute.edu.ua/#forstudent
НЕФОРМАЛЬНА ОСВІТА Рекомендовані сертифікаційні програми, курси, посібники користувача	
Web Technologies and Security Specialization	https://www.coursera.org/specializations/codio-web-tech-security
Software Security for Web Applications	https://www.coursera.org/learn/codio-software-security-for-web-applications
Network Security	https://www.coursera.org/learn/network-security
Stanford CS 253 Web Security	https://web.stanford.edu/class/cs253/
ПОЛІТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ:	
Відвідування лекційних та лабораторних занять: відвідування	Відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).
Відпрацювання пропущених занять:	відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 Office Teams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).
Правила поведінки під час занять	обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчально матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття. Задля зручності, дозволяється використання ноутбуків та інших електронних пристроїв під час навчання в комп'ютерних аудиторіях (за взаємною згодою всіх учасників освітнього процесу)
Політика академічної доброчесності ДТЕУ	https://knute.edu.ua/blog/read/?pid=38987&uk