921

68-12/П21

КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ 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

ЗАТВЕРДЖЕНО
вченою радою КНТЕУ
(прот. п. 9 від «23» 12 2021 р.)
Ректор
_____ А. А. Мазаракі

ТЕХНОЛОГІЇ БЕЗПЕКИ WEB-РЕСУРСІВ /
WEB RESOURCE SECURITY TECHNOLOGIES

ПРОГРАМА /
COURSE SUMMARY

Київ 2021

Автори: М.В. САШНЬОВА, кандидат технічних наук, доцент, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Н.О. КОТЕНКО, кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Т.О. ЖИРОВА, кандидат педагогічних наук, доцент кафедри інженерії програмного забезпечення та кібербезпеки
К.В. СТЕПАШКІНА, асистент кафедри інженерії програмного забезпечення та кібербезпеки

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки «01» листопада 2021р., протокол № 10.

Рецензенти: А.М. ДЕСЯТКО, PhD, доцент кафедри інженерії програмного забезпечення та кібербезпеки
Б.Т. БЕБЕШКО, Senior Software Engineer Softorino Ltd.

ТЕХНОЛОГІЇ БЕЗПЕКИ WEB-РЕСУРСІВ / WEB RESOURCE SECURITY TECHNOLOGIES

ПРОГРАМА / COURSE SUMMARY

ВСТУП

Програма дисципліни «Технології безпеки WEB-ресурсів» призначена для студентів другого «магістерського» рівня вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека», спеціалізації «Безпека систем електронних комунікацій в економіці», спеціальності 121 «Інженерія програмного забезпечення», спеціалізації «Інженерія програмного забезпечення».

Програму підготовлено відповідно до Стандарту вищої освіти України за даною спеціальністю та відповідної освітньо-професійної програми підготовки бакалаврів.

Програма складається з таких розділів:

1. Мета, завдання та предмет дисципліни.
2. Передумови вивчення дисципліни як вибіркової компоненти освітньої програми
3. Результати вивчення дисципліни.
4. Зміст дисципліни.
5. Список рекомендованих джерел.

1. МЕТА, ЗАВДАННЯ ТА ПРЕДМЕТ ДИСЦИПЛІНИ

Метою викладання навчальної дисципліни «Технології безпеки WEB-ресурсів» є формування у майбутніх спеціалістів умінь та компетенцій для оцінювання та забезпечення необхідного рівня захищеності Web-ресурсів, вивчення атак у вебпросторі та усунення їх наслідків.

Завданням дисципліни є формування теоретичних знань та практичних навичок з питань захисту вебзастосунків, починаючи з етапів розвідки та пошуку вразливостей, типових вразливостей серверної та клієнтської частини вебзастосунків, а також формування навичок пошуку та виправлення проблем кодування на сайті/вебзастосунку. *Знання:* міжнародних та державні стандарти по забезпеченню безпеки Web-ресурсів; існуючих Web-загроз відповідно до міжнародних та державних стандартів по забезпеченню безпеки Web-ресурсів; основ методів адміністрування інструментів дослідження вразливостей Web-ресурсів. *Вміння:* проводити оцінку наявності вразливостей та пошук вразливостей у вебзастосунках (SQL-ін'єкції, XSS, CSRF, buffer overflow, тощо); проводити аудит процесів інформаційної безпеки щодо захисту Web-ресурсів від сучасних загроз; проводити моніторинг та контроль вторгнень за допомогою інструментів тестування.

Предметом навчальної дисципліни є теорія і методологія захисту Web-ресурсів на етапах їх розробки та експлуатації.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

знання:

- «Інформаційні технології у професійній діяльності»;
- «WEB-дизайн та WEB-програмування»;

вміння:

- працювати з офісними додатками Microsoft;
- працювати з хмарними сервісами Office 365;
- працювати з пошуковою системою Google;
- використовувати основні елементи та створювати програми початкового рівня за допомогою мови програмування Python.

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Технології безпеки WEB-ресурсів», як обов'язкова компонента освітньої програми, забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідною освітньо-професійною програмою підготовки магістрів зі спеціальності «Кібербезпека»:

✓ ***«Безпека систем електронних комунікацій в економіці»***
(ОС магістр, ОП 2022 р.)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
КЗ-1	Здатність застосовувати знання у практичних ситуаціях.	1-11
КЗ-2	Здатність проводити дослідження на відповідному рівні.	1-11
КЗ-4	Здатність оцінювати та забезпечувати якість виконуваних робіт.	1-11
Фахові компетентності за освітньою програмою		
КФ1	Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і	3-11

	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.	1-2
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.	1-11
КФ6	Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.	3-11
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.	3-11
Програмні результати навчання за освітньою програмою		
РН4	Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.	3-11

РН6	Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.	3-11
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.	1-2
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.	3-11
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.	3-11
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.	2-11
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.	3-11
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.	1-11

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.	1-11
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.	1-11
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.	1-11

✓ ***«Інженерія програмного забезпечення»***
(ОС магістр, ОП 2022 р.)

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
ЗК01	Здатність до абстрактного мислення, аналізу та синтезу	1-11
Фахові компетентності за освітньою програмою		
СК01	Здатність аналізувати предметні області, формувати, класифікувати вимоги до програмного забезпечення	3-11
СК05	Здатність розробляти, аналізувати та застосовувати специфікації, стандарти, правила і рекомендації в сфері інженерії програмного забезпечення	1-2

СК07	Здатність критично осмислювати проблеми у галузі інформаційних технологій та на межі галузей знань, інтегрувати відповідні знання та розв’язувати складні задачі у широких або мультидисциплінарних контекстах.	1-11
Програмні результати навчання за освітньою програмою		
РН01	Знати і застосовувати сучасні професійні стандарти і інші нормативно-правові документи з інженерії програмного забезпечення.	1-2
РН02	Оцінювати і вибирати ефективні методи і моделі розроблення, впровадження, супроводу програмного забезпечення та управління відповідними процесами на всіх етапах життєвого циклу.	3-11
РН05	Розробляти, аналізувати, обґрунтовувати та систематизувати вимоги до програмного забезпечення.	1-11
РН07	Аналізувати, оцінювати і застосовувати на системному рівні сучасні програмні та апаратні платформи для розв’язання складних задач інженерії програмного забезпечення.	3-11
РН12	Приймати ефективні організаційно-управлінські рішення в умовах невизначеності та зміни вимог, порівнювати альтернативи, оцінювати ризики.	1-11

4. ЗМІСТ ДИСЦИПЛІНИ

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.

Список рекомендованих джерел

Основний: 1, 2
Додатковий: 6, 7, 8
Інтернет-джерела: 10, 11, 12, 13, 19

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.

Список рекомендованих джерел

Основний: 3
Додатковий: 6
Інтернет-джерела: 10, 14, 15, 19

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.

Список рекомендованих джерел

Основний:3, 4, 5
Додатковий: 6, 9
Інтернет-джерела: 10, 15, 16

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).

Список рекомендованих джерел

Основний: 3, 4
Додатковий: 6, 9
Інтернет-джерела: 10, 15, 16

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.

Список рекомендованих джерел

Основний: 3, 4
Додатковий: 6, 9
Інтернет-джерела: 10, 15, 16

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.

Список рекомендованих джерел

Основний: 3, 4
Додатковий: 6, 9
Інтернет-джерела: 10, 15, 16

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.

Список рекомендованих джерел

Основний: 3, 4
Додатковий: 6, 9
Інтернет-джерела: 10, 15, 16

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.

Список рекомендованих джерел

Основний: 3, 4
Додатковий: 6, 9
Інтернет-джерела: 10, 15, 16

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.

Список рекомендованих джерел

Основний: 3, 4
Додатковий: 6, 9
Інтернет-джерела: 10, 15, 16

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.

Список рекомендованих джерел

Основний:3, 4
Додатковий: 6, 9
Інтернет-джерела: 10, 15, 16

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 рекомендованих джерел

Основний:4
Додатковий: 7, 8, 9
Інтернет-джерела: 17, 18, 20

5. СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

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. – 218 с.

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. Elie Saad, Rick Mitchell. Owasp Testing Guide v4. Open Web Application Security Project, 2015. - 453 Pages.

4. Andrew Homan. Web Application Security Exploitation and Countermeasures for Modern Web Applications. United States of America, 2020. – 331 Pages.

5. Justin Clarke. SQL Injection Attacks and Defense. Syngress Publishing, Inc., Elsevier, Inc., 2009 - 494 Pages.

Додатковий

6. Kimberly Graves. Certified Ethical Hacker Study Guide. Wiley Publishing, Inc., Indianapolis, Indiana, 2010. - 439 Pages.

7. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Посібник]. /В.Л. Бурячок, С.В. Толюпа, В.В. Семко, Л.В. Бурячок, П.М. Складанний, Н.В. Лукова-Чуйко / –К.: ДУТ - КНУ, 2016. –178 с.

8. Bertino E., Martino L.D., Paci F., Squicciarini A.C. Security for Web Services and Service Oriented Architectures Springer, 2010. –231 p.

9. Хорошко О.В. Захист систем електронних комунікацій: навч.посіб./ В.О. Хорошко, О.В. Криворучко, М.М. Браіловський та ін. – Київ: Київ. нац. торг.-екон. ун-т, 2019. – 164 с.

Інтернет-джерела

10. The Open Web Application Security Project® (OWASP) - foundation that works to improve the security of software. URL: https://owasp.org/

11. ISO/IEC 27001:2013. Information Technology. Security Techniques. Information Security Management Systems. Requirements.
URL: https://www.certification.ua/wp-content/uploads/2018/03/ISO_27001_2013_%D0%9C%D0%9D%D0%A1-%D0%93%D0%A0%D0%A3%D0%9F%D0%9F.pdf

12. National Institute of Standards and Technology.
URL: https://nvd.nist.gov/vuln-metrics/cvss

13. Holistic Info-Sec for Web Developers.
URL: https://holisticinfosecforwebdevelopers.com/
14. Welcome to the OWASP Top 10 – 202.
URL: https://owasp.org/Top10/
15. OWASP Top 10. URL: https://tryhackme.com/room/owasptop10
16. OWASP Top 10.Course. URL: https://www.cybrary.it/course/owasp/
17. Website Security. How to Secure & Protect Your Website.
URL: https://sucuri.net/guides/website-security/
18. Як захистити веб-додатки: основні поради, інструменти, корисні посилання. URL: https://echo.lviv.ua/dev/6231
19. Національний інститут стандартів і технологій.
URL: https://www.nist.gov/
20. Free website security check & malware scanner (дослідження загроз, база даних сигнатур шкідливих програм і статистика).
URL: https://sitecheck.sucuri.net/

**Курсивом зазначені джерела, що є в наявності в бібліотеці КНТЕУ*