Силабус освітнього компонента
Програма навчальної дисципліни

Spring Security для розробників кліент-серверних додатків"

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Освітньо-професійна програма Кібербезпе

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Професійна підготовка, Вибіркова

Семестр
2

Мова викладання
Українська

Викладачі, розробники

КОРОЛЬОВ Роман Володимирович
korolevrv01@ukr.net
Кандидат технічних наук, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 80, з них патентів на корисну модель 12, 1 колективна монографія, 2 навчальних посібника, 65 статті у закордонних виданнях та фахових виданнях України, з них 5 у наукометричній базі Scopus. Провідний лектор з дисциплін: «Бездротова та мобільна безпека», «Основи стеганографії», «Бізнес інтелліджене» , «Фізичні основи технічних засобів розвідки» у студентів бакалавріата та магістратури.
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна " Spring Security для розробників кліент-серверних додатків" є вибірковою навчальною дисципліною. Дисципліна спрямована на підвищення рівня розробників, які використовують фреймворк Spring для створення корпоративних програм. Дисципліна включає розгляд потужного і гнучкого фреймворка для забезпечення безпеки в додатках, що розробляються на платформі Java з використанням Spring, який надає рішення для автентифікації (authentication) та авторизації (authorization) і є важливою частиною екосистеми Spring.

Мета та цілі дисципліни

Отримання студентами необхідних знань для забезпечення захисту веб-додатків та сервісів, зокрема через реалізацію механізмів автентифікації (перевірки особи користувача) та авторизації (управління доступом до ресурсів на основі прав та ролей користувача.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ–4. Здатність спілкуватися державною мовою як усно, так і письмово.
КЗ–6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ФК-2. Здатність аналізувати та визначати політику та стратегії забезпечення захисту інформації.

Результати навчання

РН-6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки.
РН–10. Вміти аналізувати виклики та загрози національній безпеці за напрямами професійної діяльності та синтезувати інформацію щодо розроблення та реалізації стратегій у визначальних сферах національної безпеки (політичній, економічній, соціальній, гуманітарній).
РН–19. Вміти використовувати у професійній діяльності методи та інструменти організації соціальної взаємодії, співробітництва та розв'язання конфліктів у сфері професійної діяльності, практичні навички, тактику та прийоми, роботи з людьми в інтересах службової діяльності: працювати у команді з позицій лідера, радника (консультанта), помічника, планувати використання часу та визначати стимули і бар'єри ефективної роботи, здійснювати розподіл (делегування) функцій, повноважень і відповідальності між виконавцями.
РН-21. Вміти застосовувати теорії та методи захисту для забезпечення безпеки елементів об'єктів критичної інфраструктури, кіберфізичних систем та інформаційно- комунікаційних систем.
РН-22. Вміти застосовувати національні та міжнародні регулятори в сфері інформаційної безпеки щодо розслідування комп'ютерних інцидентів.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 32 год., лабораторні роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Безпека Інтернет речей та сервісів, Мережева та хмарна безпека, Безпека систем Клієнт-Сервер.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Теми лекційних занять

Тема 1. Поширені вразливості безпеки у веб-додатках. Вразливості в автентифікації та авторизації.
Міжсайтовий скриптинг (XSS), підробка міжсайтових запитів (CSRF). Ін'єкції у веб-додатках. Вирішення проблеми розкриття конфіденційних даних.
Тема 2. Керування користувачами.
Реалізація автентифікації у Spring Security . Опис користувача.
Тема 3. Робота з паролями.
Визначення контракту PasswordEncoder. Модуль Spring Security Crypto. Використання генераторів ключів.
Тема 4. Реалізація автентифікації.
Представлення запиту під час автентифікації. Використання контексту безпеки. Використання та налаштування HTTP Basic.
Тема 5. Налаштування авторизації: Обмеження доступу.

Обмеження доступу на основі повноважень і ролей. Обмеження доступу для всіх кінцевих точок на основі повноважень користувачів. Обмеження доступу для всіх кінцевих точок на основі ролей користувачів. Обмеження доступу до всіх кінцевих точок.

Тема 6. Налаштування повноважень: Застосування обмежень.

Використання методів відповідності для вибору кінцевих точок. Вибір запитів на авторизацію з використанням MVC matchers. Вибір запитів на авторизацію з використанням Ant matchers. Відбір запитів на авторизацію з використанням regex.

Тема 7. Реалізація фільтрів.

Реалізація фільтрів в архітектурі Spring Security архітектурі Spring Security. Реалізації фільтрів, надані Spring Security.

Тема 8. Застосування CSRF-захисту та CORS.

Застосування захисту від підробки міжсайтових запитів (CSRF) в додатках. Використання спільного використання ресурсів різного походження.

Тема 9. Структура OAuth 2.

Компоненти автентифікації OAuth 2. Варіанти реалізації за допомогою OAuth.

Тема 10. OAuth 2: Використання JWT та криптографічних підписів.

Використання токенів, підписаних симетричними ключами, з JWT. Використання токенів, підписаних асиметричними ключами, з JWT. Додавання користувацьких даних до JWT.

Тема 11. Глобальна безпека методу.

Увімкнення безпеки глобальних методів. Застосування попередньої авторизації для повноважень та ролей. Застосування післяавторизації. Впровадження дозволів для методів.

Тема 12. Spring Security для реактивних програм.

Що таке реактивні програми. Керування користувачами у реактивних програмах. Налаштування правил авторизації у реактивних програмах. Застосування авторизації на рівні кінцевих точок у реактивних програмах.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Налаштування UserDetailsService і PasswordEncoder.

Тема 2. Розробка захищеного веб-додатку.

Тема 3. Реєстрація та авторизація за допомогою Spring Security.

Самостійна робота

Самостійна робота студента є однією з форм організації навчання, основною формою оволодіння навчальним матеріалом у вільний від аудиторних навчальних занять час. Під час самостійної роботи студенти вивчають лекційний матеріал, готуються до лабораторних робіт, контрольних робіт, заліків та іспитів. Студентам також рекомендуються додаткові матеріали (відео, статті) для самостійного вивчення та аналізу.

Неформальна освіта

В рамках неформальної освіти згідно відповідного Положення (http://surl.li/pxssv), освітня компонента або її окремі теми можуть бути враховано у разі самостійного проходження професійних курсів/тренінгів, отримання громадянської освіти, онлайн освіти, професійного стажування тощо.

За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література та навчальні матеріали

Основна література

1. Laurentiu Spilca Spring Security in Action. – Shelter Island: 2020. - 560 с. [Електронний ресурс]. – Режим доступу:

https://books.google.com.ua/books?id=CF4BEAAAQBAJ&printsec=frontcover&redir_esc=y#v=onepage&q&f=false
2. Carnell John. Spring Microservices in Action Packt Publishing, 2017. — 384 p. [Електронний ресурс]. – Режим доступу: https://hoclaptrinhdanang.com/downloads/pdf/spring/Spring%20Microservices%20in%20Action.pdf

Додаткова література

3. Spring-security [Електронний ресурс]. – Режим доступу: https://spring.io/projects/spring-security
4. Spring-security [Електронний ресурс]. – Режим доступу: https://www.manning.com/books/spring-security-in-action

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•лабораторні роботи: 40% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% семестрової оцінки;
•залік: 40% семестрової оцінки.

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D
60–63	Задовільно	E
35–59	Незадовільно (потрібне додаткове вивчення)	FX
1–34	Незадовільно (потрібне повторне вивчення)	F

Норми академічної етики і політика курсу

Студент повинен дотримуватися «Кодексу етики академічних взаємовідносин та доброчесності НТУ «ХПІ»: виявляти дисциплінованість, вихованість, доброзичливість, чесність, відповідальність. Конфліктні ситуації повинні відкрито обговорюватися в навчальних групах з викладачем, а при неможливості вирішення конфлікту – доводитися до відома співробітників дирекції інституту. Нормативно-правове забезпечення впровадження принципів академічної доброчесності НТУ «ХПІ» розміщено на сайті: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Погодження

Силабус погоджено	28.08.2024		Завідувач кафедри Сергій ЄВСЕЄВ
	28.08.2024		Гарант ОП Ольга КОРОЛЬ