Силабус освітнього компонента
Програма навчальної дисципліни

Комплексний тренінг «Безпека веб-застосунків»

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій (320)

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Магістр

Тип дисципліни
Профільна підготовка, Вибіркова

Семестр
2

Мова викладання
Українська

Викладачі, розробники

Король Ольга Григорівна

olha.korol@khpi.edu.ua
Кандидат технічних наук, доцент, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 161, з них патентів на корисну модель 18, 11 монографій, з яких 6 колективних монографій, 18 навчальних посібників, 66 статті у закордонних виданнях та фахових виданнях України, у тому числі у наукометричній базі Scopus. Провідний лектор з дисциплін: «Основи соціальної інженерії», «Інформаційна безпека держави», «Менеджмент інформаційної безпеки», «Організація документообігу з обмеженим доступом», «Безпека в соціальних мережах».
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Комплексний тренінг «Безпека веб-застосунків»" є вибірковою навчальною дисципліною. Складність розроблюваних веб-застосунків зростає з кожним роком, що, в свою чергу, робить важкоздійсненним забезпечення їхньої безпеки. Саме тому, доцільно приділяти особливу увагу критичним проблемам захисту програмного забезпечення. Вміння оцінювати ризики та запобігати вразливостям ще на етапі проектування продукту є вкрай важливою задачею, котра знижує потенційні складності при експлуатації застосунку.

Мета та цілі дисципліни

Формування практичних навичок щодо виявлення та протидії сучасним загрозам в кіберпросторі на основі відпрацювання практичних завдань.

Формат занять

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

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
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.

Результати навчання

РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН3. Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
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.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
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.
РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес\операційних процесів у сфері інформаційної та\або кібербезпеки в цілому.
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.
РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
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.
РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
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.

Обсяг дисципліни

Загальний обсяг дисципліни 150 год. (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Веб-безпека , Бездротова та мобільна безпека, Тестування на проникнення та етичний хакінг.

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. Впровадження коду.
Виявлення ін’єкцій, таких як SQL, NoSQL, ОС та ін’єкція LDAP, які виникають, коли ненадійні дані надсилаються інтерпретатору як частина команди чи запиту.
Тема 2. Некоректна автентифікація і управління сесією.
Виявлення функцій іплікації, які пов’язані з автентифікацією та керуванням сеансом, що дозволяє зловмисникам компрометувати паролі, ключі або скельні маркери або використовувати інші недоліки впровадження, щоб тимчасово або назавжди припустити особистість інших користувачів.
Тема 3. Міжсайтовий скриптинг (XSS).
Виявлення веб-додатків та API, які не захищені належним чином. Зловмисники можуть вкрасти або змінити такі слабко захищені дані, щоб вчинити шахрайство з кредитною карткою, крадіжку особи або інші злочини.
Тема 4. Небезпечні прямі посилання на об’єкти.
Аналіз старих або погано налаштованих процесорів XML оцінюють посилання зовнішніх об'єктів у документах XML. Зовнішні об’єкти можуть використовуватися для розкриття внутрішніх файлів за допомогою обробника URI файлів, обміну внутрішніми файлами, сканування внутрішніх портів, віддаленого виконання коду та відмови в атаці служби.
Тема 5. Небезпечна конфігурація.
Аналіз обмеження щодо дозволених користувачів, які дозволено робити, часто не виконуються належним чином. Зловмисники можуть використовувати ці недоліки для доступу до несанкціонованих функціональних можливостей та / або даних, таких як доступ до облікових записів інших користувачів, перегляд конфіденційних файлів, зміна даних інших користувачів, зміна прав доступу тощо.
Тема 6. Витік чутливих даних – оцінка конфігурації безпеки.
Зазвичай це результат небезпечних конфігурацій за замовчуванням, неповних або спеціальних конфігурацій, відкритого хмарного сховища, неправильно налаштованих заголовків HTTP та багатослівних повідомлень про помилки, що містять конфіденційну інформацію. Не тільки всі операційні системи, рамки, бібліотеки та додатки повинні бути надійно налаштовані, але вони повинні бути виправлені / модернізовані своєчасно.
Тема 7. Відсутність контролю доступу до функціонального рівня.
Визначення недоліків XSS, які виникають щоразу, коли програма включає недовірені дані на новій веб-сторінці без належної валідації або не відкриття, або оновлює наявну веб-сторінку за допомогою наданих користувачем даних за допомогою API браузера, який може створювати HTML або JavaScript. XSS дозволяє зловмисникам виконувати скрипти в браузері жертви, які можуть захоплювати сеанси користувачів, знищувати веб-сайти або перенаправляти користувача на шкідливі сайти.

Тема 8. Підробка міжсайтових запитів (CSRF).
Оцінка небезпечної десеріалізації, яка часто призводить до віддаленого виконання коду. Навіть якщо дефери дезаріалізації не призводять до віддаленого виконання коду, їх можна використовувати для виконання атак, включаючи атаки відтворення, атаки ін'єкції та напади ескалації привілеїв.
Тема 9. Використання компонентів з відомими уразливостями.
Аналіз компонент, таких як бібліотеки, рамки та інші програмні модулі, які працюють із тими ж привілеями, що і додаток. Якщо використовується вразливий компонент, така атака може полегшити серйозні втрати даних або захоплення сервера. Програми та API, що використовують компоненти з відомою вразливістю, можуть підірвати захисні програми та включити різні атаки та впливи.
Тема 10. Невалідовані редіректи.
Виявлення недостатнього обліку та моніторингу у поєднанні з відсутньою або неефективною інтеграцією з реакцією на інцидент дозволяє зловмисникам надалі атакувати системи, підтримувати стійкість, перетворювати на більші кількості систем, а також підробляти, витягувати або знищувати дані. Більшість досліджень щодо порушення виявляють час виявлення порушення понад 200 днів, як правило, виявляються зовнішніми сторонами, а не внутрішніми процесами чи моніторингом.

Теми практичних занять

Практичні роботи в рамках дисципліни не передбачені.

Теми лабораторних робіт

Тема 1. Впровадження коду.
Тема 2. Некоректна автентифікація і управління сесією.
Тема 3. Міжсайтовий скриптинг (XSS).
Тема 4. Небезпечні прямі посилання на об'єкти.
Тема 5. Небезпечна конфігурація.
Тема 6. Витік чутливих даних – оцінка конфігурації безпеки.
Тема 7. Відсутність контролю доступу до функціонального рівня.
Тема 8. Підробка міжсайтових запитів (CSRF).
Тема 9. Використання компонентів з відомими уразливостями.
Тема 10. Невалідовані редіректи.

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 та заліку.

Література та навчальні матеріали

Основна література:

1. Kali Linux Web Penetration Testing Cookbook, Second Edition (Packt Publishing) URL: https://www.packtpub.com/product/kali-linux-web-penetration-testing-cookbook-second-edition/9781788991513.
2. Зразок звіту з тестування на проникнення URL: https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf.
3. Зразок технічного звіту з проникнення URL: https://tbgsecurity.
4. OWASP Top 10: issues in the 10 most critical security risk categories in your web applications URL: https://www.sonarqube.org/features/security/owasp/ ?gads_campaign=Europe-1-Generic&gads_ad_group=OWASP& gads_keyword=owasp%20top%2010&gclid=CjwKCAiAsNKQBhAPEiwAB-I5zQywzTKai6fcrilMphlAn21CRehrI0q9DEjUZNpHUoDt5V_bVpLm4RoClIkQAvD_BwE.

5. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
6. WEB-технології [Електронний ресурс]: Навчально-довідковий посібник / С.П. Євсеєв, А.М. Ткачов, В.О. Алексієв, Ю.М. Рябуха – Харків : ХНЕУ ім. С. Кузнеця, – Львів: Видавництво «Новий Світ –2000», 2021. – 390 с.

Додаткова література :

1 Встановлення Metasploitable 2 URL: https://metasploit.help.rapid7.com/docs/metasploitable-2.
2. Збірка Metasploitable 3 URL: https://github.com/rapid7/metasploitable3.
3. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
4. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
5. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.

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: 20% семестрової оцінки;
- залік: 30% 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 28.08.2023 — Завідувач кафедри Сергій ЄВСЕЄВ

28.08.2023 — Гарант ОП Олександр МІЛОВ