КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ

ІМЕНІ БОРИСА ГРІНЧЕНКА

Факультет інформаційних технологій та математики

Кафедра інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

Затверджено на засіданні кафедри
інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка
(протокол № 5 від 03.04.24)

РОБОЧА ПРОГРАМА ІСПИТУ

ТЕХНОЛОГІЇ БЕЗПЕКИ WEB-РЕСУРСІВ

галузь знань	12 Інформаційні технології
спеціальність	125 Кібербезпека та захист інформації
освітня програма	125.00.01 Безпека інформаційних і комунікаційних систем

2023-2024 навчальний рік

Опис програми іспиту

Київський столичний університет імені Бориса Грінченка

Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

Програма іспиту з дисципліни
«Технології безпеки Web-ресурсів»

1 курс – освітній рівень – другий (магістерський)

Спеціальність 125 Кібербезпека та захист інформації

Освітня програма: 125.00.01 Безпека інформаційних і комунікаційних систем

Форма проведення: тестування на платформі Moodle в ЕНК дисципліни: https://elearning.kubg.edu.ua/course/view.php?id=21872

Тривалість проведення **1 год. 20 хв.**

Максимальна кількість балів: **40 балів**

Екзамен проводиться в університетській аудиторії у тестовій формі із використанням персональних комп'ютерів, якщо ситуація дозволяє проведення освітнього процесу офлайн. Якщо ж освітній процес проходить дистанційно, то екзамен проводиться онлайн в режимі відеоконференції засобами Google Meet.

Форма проведення екзамену – комбінована. Екзамен оцінюється у 40 балів за розподілом: 20 балів – комплексний комп'ютерний тест з дисципліни; 20 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями.

Оцінювання практичного завдання відбувається в межах від 0 до 20 балів, згідно критеріїв оцінювання.

Критерії оцінювання практичного завдання (задачі):

20-17 балів: Відмінний рівень умінь, розв'язання задачі повне, вичерпне володіння програмним забезпеченням, можливими, незначними недоліками

16-13 балів: Добрий рівень умінь, розв'язання задачі містить небагато недоліків та / або незначну кількість помилок

12-9 балів: Мінімально допустимий рівень умінь, що характеризується недостатнім рівнем володіння програмним забезпеченням, розв'язання задачі неповне, містить недоліки та помилки

8-5 бали: Незадовільний рівень умінь, що виявляється у нездатності застосувати знання при розв'язанні задач.

4-1 бал: Незадовільний рівень умінь, що виявляється у неспроможності володіння програмним забезпеченням, невмінні розв'язувати задачі.

0 балів: Відповідь відсутня.

Екзамен проводиться із суворим дотриманням принципів академічної доброчесності, що передбачає недопустимість списування, фальсифікацій та обману. При порушенні студент відсторонюється від подальшого проходження екзаменаційного тесту із підсумковою оцінкою Fx за дисципліну. При виконанні завдань допускається користування довідковою літературою, таблицями значень функції, критеріїв та ін.

Підсумкова оцінка в балах (максимально 100 балів) за дисципліну є сумою результату поточного контролю за семестр (60 балів) та відповіді на екзамені (40 балів).

Перелік тем, які виносяться на іспит:

1. Протокол передачі гіпертексту.
2. HTTP-запити та відповіді, методи та повідомлення.
3. Кукі.
4. HTTPS (протокол передачі гіпертексту через захищені сокети).
5. Протокол SSL (Secure Sockets Layer).
6. Симетричне та асиметричне шифрування.
7. Перехоплення проксі та HTTPS.
8. Використання протоколу простого доступу до об’єктів (SOAP).
9. Протокол SMTP (Simple Mail Transfer Protocol).
10. Протокол поштового відділення (POP3).
11. Протокол доступу до Інтернету (IMAP).
12. Архітектура веб-систем і веб-додатків.
13. Об’єкти захисту/атаки.
14. Класифікація веб-атак (уразливості).
15. Груба сила (Brute Force).
16. Недостатня аутентифікація.
17. Недостатнє відновлення пароля (перевірка слабкого відновлення пароля).
18. Прогнозування вхідних даних/сеансів.
19. Недостатня авторизація.
20. Недостатнє закінчення сеансу.
21. Фіксація сеансу.
22. Викрадення сеансу.
23. Перехресні сценарії (XSS).
24. Сценарії крос-кадрів (XFS) або iframe-ін’єкція.
25. Підробка запитів на місцях, CSRF.
26. Зловживання JSON.
27. Переповнення буфера.
28. LDAP-ін’єкція.
29. SQL-ін’єкція.
30. SSI-ін’єкція.
31. XPath-ін’єкція.
32. Індексування каталогів.
33. Витоки інформації.
34. Пошук шляху (трасування).
35. Передбачуване розташування ресурсів.
36. Забезпечення технологій веб-додатків (SWAT).
37. Обробка помилок та ведення журналу.
38. Аутентифікація.
39. Обробка вхідних і вихідних даних.
40. Конфігурація та операції.
41. Управління сеансами.
42. Контроль доступу.
43. Про проект тестування OWASP.
44. Принципи тестування.
45. Пояснення техніки тестування.
46. Виведення вимог до тестування безпеки.
47. Тести безпеки, інтегровані в робочі процеси розробки та тестування.
48. Аналіз і звітність тестових даних безпеки.

49. Інструменти тестування.
50. Основні поняття аудиту веб-додатків.
51. Методика організації та проведення аудиту веб-додатків.

Екзаменатор  Володимир СОКОЛОВ

Завідувач кафедри  Павло СКЛАДАННИЙ