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 № 11 від 15.10.2024)

РОБОЧА ПРОГРАМА ІСПИТУ

БЕЗПЕКА WEB РЕСУРСІВ

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

2024-2025 навчальний рік

Опис програми іспиту

Київський столичний університет імені Бориса Грінченка
Кафедра інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Програма іспиту з дисципліни «Безпека Web ресурсів»
3 курс – освітній рівень – перший (бакалаврський)
Спеціальність 125 Кібербезпека
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=20351
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. Студент дає відповіді на запитання електронного тесту в системі Moodle. Тест містить 30 тестових питань закритого типу (вибір правильної відповіді із запропонованих варіантів), які передбачають автоматичну (комп'ютерну) перевірку і оцінюються по 1-2 бали кожне. 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. 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. Навіщо нам потрібна безпека в Інтернеті. 2. Огляд топ-10 списку OWASP. 3. Приклад вразливого веб-сайту. 4. Використання Chrome's/Firefox інструментів для розробників. 5. Моніторинг та складання запитів за допомогою Fiddler. 6. Модифікація запитів та відповідей у Fiddler. 7. Захист транспортного рівня. 8. Поняття атаки «людини посередині». 9. Захист конфіденційної інформації підчас її пересилання. 10. Ризик надсилання файлів cookies через незахищені з'єднання. 11. Чому завантажувати форми для входу HTTP є ризикованим. 12. Використання вмісту змішаного режиму. 13. Заголовок HSTS. 14. Основні поняття JavaScript.

15. Основні поняття PHP.
16. Серверна сторона VS.
17. Клієнтські мови.
18. Виявлення ненадійної інформації та її ліквідація.
19. Встановлення сигналів для використання практик ліквідації.
20. Поняття XSS та вихідних даних; визначення обставин використання вихідних даних.
21. Доставка інформації через відображений XSS.
22. Тестування ризиків стійкості XSS.
23. Заголовок X-XSS-Захист.
24. Cookies 101.
25. Поняття Http лише cookies.
26. Поняття безпечних cookies.
27. Прядок налаштування клієнта OpenVPN на Windows.
28. Обмеження доступу файлів cookie задаванням шляху.
29. Зниження ризику у зв'язку із закінченням терміну дії файлів cookie.
30. Використання тимчасових cookies для подальшого зменшення ризиків.
31. Порядок налаштування VPN з'єднання и сервера на Windows 10, 8, 7.
32. Як зловмисник створює профіль ризику на веб-сайті.
33. Поняття заголовку відповіді сервера.
34. Розміщення ризикованих веб-сайтів.
35. «Відбитки пальців» HTTP серверів.
36. Розкриття інформації через robots.txt.
37. Ризики в джерелах HTML.
38. Внутрішнє повідомлення про помилку.
39. Форми використання NAT.
40. Відсутність засобів контролю діагностичних даних.
41. Ідентифікація ненадійних даних у параметрах запитів HTTP.
42. Захоплення запитів та маніпулювання параметрами.
43. Маніпулювання логікою програми за допомогою параметрів.
44. Тестування відсутності перевірки з боку сервера.
45. Розуміння побудови моделі.
46. Приведення в дію атаки масового призначення.
47. Маніпуляція HTTP заголовками. Fuzz-тестування; вразливість при завантаженні файлу.
48. Local file inclusion (LFI). Remote File Inclusion (RFI).
49. Складові SQLi атак – небезпечні введення та помилки серверу.
50. Складові SQLi атак – назви таблиць та колонок, отримання дійсних облікових даних для сайту.
51. Типи SQL вводу: параметризовані запити та збережені процедури, уникнення введення команд користувача, обмеження привілеїв, перевірка білого списку.
52. Тестування ризикованих рішень. Дослідження структури бази даних за допомогою введення даних.
53. Збирання даних за допомогою введення інформації.
54. Автоматизація атак з "Havij" або "Sqlmap".

55. Сліпе SQL введення даних; безпечні моделі додатків. Особливості побудови мережі з proxy-сервером.
56. Що таке XSRF?
57. Вивчення за прикладом - XSRF з GET та POST параметрами.
58. XSRF введення даних – референт, заголовок джерела та відповідь на виклик.
59. XSRF введення даних – маркер синхронізатора.
60. Поняття cross site атак.
61. Тестування ризику підробки cross site; роль anti-forgery знаків; тестування підробки cross site запитів проти APIs.
62. Встановлення атаки кликджекингу.
63. Поняття міцності паролю та векторів атаки. Обмеження введення символів у паролях.
64. Надсилання облікових даних для створення облікових записів.
65. Перерахування рахунку.
66. Відмова від сервісу за допомогою оновлення паролю.
67. Забезпечення правильного оновлення паролю; встановлення небезпечного зберігання паролів.
68. Тестування ризиків у функції «запам’ятати мене».
69. Повторне підтвердження перед ключовими діями.
70. Тестування брутфорс автентифікації. Тестування незахищеної captcha.

Приклад екзаменаційного завдання

Які з перерахованих нижче варіантів є найбільш вразливими для атак? Оберіть декілька відповідей.

a. Session ID
b. Registry keys
c. Regular expressions
d. SQL queries based on user input

Екзаменатор  Махіяр ТАДЖДІНІ

Завідувач кафедри  Павло СКЛАДАННИЙ