**Вопросы для экзамена по дисциплине «Практические аспекты информационной безопасности»**

**Часть 1. Исследование безопасности веб-приложений**

1. Базовые методы анализа безопасности веб-приложений.

2. Структура веб-приложения.

3. Финальные цели злоумышленника/исследователя.

4. План исследования веб-приложения (стратегия атаки типичного злоумышленника)

5. Первоначальный анализа, сбор информации: цели, методы, средства.

6. Дистрибутивы для анализа безопасности.

7. Базовые утилиты для анализа веб-приложения.

8. Сетевой сканер nmap.

9. Burp Suite. Принцип работы, возможности.

10. Сканер уязвимостей для веб-приложений, разработанных с помощью Wordpress.

11. Понятие уязвимости. SQLi (с примерами).

12. Понятие уязвимости. LFI (с примерами).

13. Понятие уязвимости. RCE (с примерами).

14. Заголовки HTTP.

15. Особенности PHP. Атака Request Injection.

**Часть 2. Исследование безопасности Desktop-приложений.**

1. Обратная разработка, определение, суть, конечные цели.

2. Компиляция и дизассемблирование.

3. Центральный процессор, регистры, язык ассемблера.

4. Инструменты для обратной разработки.

5. Дизассемблер IDA Pro.

6. Отладчики, примеры, предназначение.

7. Принципы архитектуры фон Неймана.

8. Выполнение программы

9. Соглашение о вызове.

10. Механизмы защиты от копирования.

11. Анализ дизассемблированных циклов.

12. Анализ дизассемблированных ветвлений.

13. Бинарные уязвимости.

14. Уязвимость переполнения буфера на стеке. Принцип уязвимости.

15. Уязвимость переполнения буфера на стеке. Техники эксплуатации.