Вопросы к экзамену по учебной дисциплине «Защита веб-ресурсов от несанкционированного доступа» (3 семестр)

1. Веб-ресурсы. Виды веб-серверов и веб-приложений. Конфигурация веб-серверов.
2. Структура веб-приложения. Процесс установки соединения по HTTP-протоколу.
3. Взаимодействие клиент-сервер. Протокол HTTP. Структура запроса клиента и ответа сервера.
4. Описание методов, использующихся в заголовках HTTP-пакета. Классы кодов состояния ответов сервера.
5. Описание атаки HTTP Spliting и способы ее реализации. Методы защиты от атаки HTTP Spliting.
6. Принципы использования кеширования при взаимодействии клиента с сервером.
7. Принцип реализации атаки Cache Poisoning и ее последствия.
8. Применение инструментов для анализа уязвимостей.
9. Серверные операционные системы. Семейство операционных систем Linux. Организация файловой системы.
10. Командная оболочка операционной системы Linux. Основные команды.
11. Управление правами пользователей в операционной системе Linux.
12. Файловая структура ОС Linux. Использование команд Linux для обнаружения уязвимостей управления доступа.
13. Назначение и функции Telnet и SSH протоколов. Процесс установки соединения клиент-сервер по SSH протоколу.
14. Отличия версий SSH-протокола. Определение SFTP-протокола и его отличия от SSH.
15. Назначение использования утилиты Netcat в сочетании с SSH-туннелем. Описать реализацию SSH-туннеля.
16. Назначение и функции утилиты Nmap. Привести примеры использования утилиты Nmap для проверки и сканирования портов.
17. Особенности установление SSH-соединения в ОС Linux.
18. Методы сбора информации о веб-ресурсе. Сканеры сетей. Применение Netcat.
19. Назначения и отличия SSL и TLS. Принцип работы SSL. Процесс рукопожатия по SSL.
20. Способы получения SSL-сертификата. Порядок осуществления соединения по TLS.

21. Утилиты для сбора информации о сервере. Назначение OpenSSL.
22. Уязвимость Renegotiation. Механизм Secure Renegotiation. Механизм Client Initiated Renegotiation.
23. Назначение и виды тестирования на проникновение. Международные стандарты.
24. Этапы тестирования на проникновение. Виды методов тестирования на проникновение.
25. Методологии тестирования.Проект обеспечения безопасности веб-приложений Open Web Application Security Project.
26. Виды баз данных. Управление базами данных. Oracle, MySQL. Языки программирования веб-приложений.
27. Базовые операторы для SQL-запросов. Взаимодействие между компонентами web-приложения на основе SQL-запросов.
28. Виды SQL-injection. Описание атаки SQL-injection, примеры реализации.
29. Основные причины возникновения SQL- инъекций в приложениях.
30. Пример динамического SQL-запроса. Техники эксплуатации SQL-инъекций. Примеры.
31. Отличия Time-based SQL-инъекция от Blind SQL-инъекцию.
32. Назначение и описание атаки Command Injection.
33. Структура веб-страниц. HTML и XML.
34. Построение HTML-документа. DOM и DTD. Теги HTML и XML. Отличия XML и HTML.
35. Назначение Cookie. Процесс установки соединения с использованием Cookie. Атрибуты Cookie.
36. Механизм реализации атаки XSS. Виды XSS-атак. Типы XSS-уязвимостей по месту выполнения.
37. Примеры использования XXS-атаки для фишинга. Атака Cross-Site Request Forgery.
38. Уязвимости XSS, вызванные кодом на стороне клиента.
39. Механизм управлением доступа. Виды управления доступом. Назначение куки, структура и атрибуты.
40. HTTP-аутентификация. Forms authentication. Аутентификация по ключам доступа.
41. Аутентификация по токенам. Форматы токенов. Использования SAML для сценария Single Sign-On. Стандарт OAuth.
42. Назначение сессии веб-приложения.
43. Атака фиксации сессии. Атака Cross-Site Request Forgery.

44. Shell-инъекция. Атаки обхода путей (директорий).
45. Определение и назначение AJAX, уязвимости AJAX.
46. DOM-инъекция, XML-инъекция,
47. Назначение и особенности FortiWeb.
48. Пояснить принцип работы FortiWeb в режиме Reverse Proxy.
49. Отличительные особенности режима Offline Protection.
50. Режимы True Transparent Proxy и Transparent Inspection.
51. Назначение WCCP режима.
52. Способы подключения к FortiWeb, особенности конфигурации подключения к серверу.
53. Назначение аутентификации пользователей на веб-ресурсе, последовательность действий при конфигурации аутентификации пользователей.
54. Принцип работы FortiWeb для защиты от разных видов атак.
55. Конфигурация защиты от веб-атак на устройстве FortiWeb.
56. Способы обнаружения SQL-инъекций устройством FortiWeb.
57. Назначение AST. Принцип защиты от Cross-Site Request Forgery.
58. Атаки LFI и RFI, способы защиты. Конфигурация защиты от DDoS атак на устройстве FortiWeb.