Состояние	Завершены
Тест начат	воскресенье, 12 октября 2025, 20:08
Завершен	воскресенье, 12 октября 2025, 20:15
Затраченное время	7 мин. 29 сек.
Баллы	30,00/30,00
Оценка	**10,00** из 10,00 (**100**%)

Вопрос 1

Выполнен

Баллов: 1,00 из 1,00

У вас на сервере установлено веб-приложение, которое отвечает на запросы по протоколу https (стандартный порт), других сетевых приложений доступных извне не предполагается. При настройке межсетевого экрана, какие порты вы оставите открытыми?

Ответ: 443

Должен остаться только стандартный порт протокола https (443).

Вопрос 2

Выполнен

Баллов: 1,00 из 1,00

Вы анализируете приложение и замечаете, что оно передает идентификатор сессии методом GET. К какой из угроз OWASP Top 10 относится подобная уязвимость? Выберите правильный вариант ответа.

Выберите один ответ:

- a. A03 Injection
- b. A04 Insecure Design
- c. A01 Broken Access Control
- d. A05 Security Misconfiguration
- e. A08 Software and Data Integrity Failures
- f. A07 Identification and Authentication Failures
- g. A02 Cryptographic Failures

Передача идентификатора сессии методом GET может с большой вероятностью привести к его утечке, и сеанс пользователя будет скомпрометирован – это ошибки аутентификации и идентификации.

Вопрос 3

Выполнен

Баллов: 1,00 из 1,00

К какой из угроз OWASP Top 10 относится уязвимость XSS? Выберите правильный вариант.

Выберите один ответ:

- a. A02 Cryptographic Failures
- b. A03 Injection
- c. A04 Insecure Design
- d. A05 Security Misconfiguration
- e. A01 Broken Access Control

Атака межсайтового скриптинга относится к классу атак через инъекции.

Вопрос 4

Выполнен

Баллов: 1,00 из 1,00

Вы две недели были в отпуске, и по возвращению включив компьютер, заметили, что ваша сессия в онлайн банке по-прежнему активна, то есть вам не надо заново проходить процедуру аутентификации на данном компьютере. Подумайте, является ли такое приложение безопасным. К какой из угроз OWASP Top 10 относится подобная уязвимость? Выберите правильный вариант ответа.

Выберите один ответ:

- a. A08 Software and Data Integrity Failures
- b. A02 Cryptographic Failures
- c. A07 Identification and Authentication Failures
- d. A01 Broken Access Control
- e. A05 Security Misconfiguration
- f. A03 Injection
- g. A06 Vulnerable And Outdated Components

Отсутствие механизмов инвалидации сессии (например, по тайм-ауту в случае неактивности пользователя) значительно повышают вероятность кражи сессии – это ошибки аутентификации и идентификации.

Вопрос 5

Выполнен

Баллов: 1,00 из 1,00

Вы в своем приложении используете сторонние библиотеки. Вы заметили, что одна из библиотек не обновлялась больше полугода. Анализируя репозиторий github для данной библиотеки, вы видите, что за последний год накопилось большое количество Issues, на которые разработчик не реагирует. Подумайте, стоит ли продолжать использовать такую библиотеку? К какой из угроз OWASP Top 10 вы бы отнесли подобную уязвимость? Выберите правильный вариант ответа.

Выберите один ответ:

- a. A03 Injection
- b. A08 Software and Data Integrity Failures
- c. A01 Broken Access Control
- d. A04 Insecure Design
- e. A06 Vulnerable and outdated components
- f. A05 Security Misconfiguration

Вопрос 6

Выполнен

Баллов: 1,00 из 1,00

Вы анализируете приложение и замечаете, что для восстановления забытого пароля система задает стандартный вопрос «укажите ваш день рожденья». Подумайте, является ли такая схема безопасной. К какой из угроз OWASP Top 10 относится подобная уязвимость? Выберите правильный вариант ответа.

Выберите один ответ:

- a. A08 Software and Data Integrity Failures
- b. A03 Injection
- c. A02 Cryptographic Failures
- d. A01 Broken Access Control
- e. A07 Identification and Authentication Failures
- f. A05 Security Misconfiguration
- g. A06 Vulnerable And Outdated Components

Слабые (уязвимые) механизмы восстановления пароля делают систему небезопасной (с точки зрения кражи учетной записи), даже если основной механизм аутентификации реализован надежно. Безопасность системы определяется безопасностью ее наиболее слабого звена – это ошибки аутентификации и идентификации.

Вопрос 7

Выполнен

Баллов: 1,00 из 1,00

К какой из угроз OWASP Top 10 относится уязвимость в системе, при которой администратор оставил стандартные пароли для дефолтных учетных записей (например, при использовании сторонних систем)? Выберите правильный вариант ответа.

Выберите один ответ:

- a. A08 Software and Data Integrity Failures
- b. A03 Injection
- c. A01 Broken Access Control
- d. A02 Cryptographic Failures
- e. A05 Security Misconfiguration
- f. A04 Insecure Design

Вопрос 8

Выполнен

Баллов: 1,00 из 1,00

Какие уязвимости относятся к классу угроз OWASP Top 10 A02 Cryptographic failures? Выберите все верные варианты.

Выберите один или несколько ответов:

- [ ] a. Использование простых паролей
- [ ] b. Межсайтовая подделка запросов
- [x] c. Несвоевременное обновление криптографических ключей
- [ ] d. Инъекция в командную строку
- [x] e. Использование предсказуемого генератора случайных чисел
- [ ] f. CSRF (cross site request forgery)
- [ ] g. Сохранение чувствительной информации в системных журналах
- [x] h. Передача чувствительных данных без шифрования
- [x] i. Использование слабых хеш-алгоритмов

К этой группе уязвимостей относятся уязвимости, связанные с применением.

Вопрос 9

Выполнен

Баллов: 1,00 из 1,00

Является ли безопасным сохранять чувствительную информацию (например, пароль для доступа к БД или учетной записи пользователя) в системных журналах?

Выберите один ответ:

- a. Да
- b. Нет

Нет, хранение чувствительной информации в журналах не рекомендуется, это ошибка Insecure Design.

Вопрос 10

Выполнен

Баллов: 1,00 из 1,00

Какие уязвимости относятся к классу угроз OWASP Top 10 A09 Security Logging and Monitoring Failures? Выберите все верные варианты.

Выберите один или несколько ответов:

- a. Отсутствие проверки целостности компонентов после загрузки
- b. Отсутствие проверок целостности в цепочках CI/CD
- c. Установка неиспользуемых библиотек и компонентов
- d. Инъекция в командную строку
- e. Межсайтовая подделка запросов
- f. CSRF (cross site request forgery)
- g. Недостаточное журналирование событий
- h. Не использование многофакторной аутентификации
- i. Сохранение пользовательского ввода в системный журнал без необходимого экранирования
- j. Запись чувствительной информации в системные журналы

К данному классу угроз относятся все угрозы, связанные с загрузкой или обновлением приложений или библиотек без проверки целостности того, что именно загружается. В случае использования автоматизированной установки, проверка должна быть встроена в автоматическую цепочку.

Вопрос 11

Выполнен

Баллов: 1,00 из 1,00

Как называется специализированное приложение, которое умеет смотреть контент http пакета и обнаружить такие атаки как XSS?

Ответ: Web Application Firewall

Вопрос 12

Выполнен

Баллов: 1,00 из 1,00

Умеет ли стандартный межсетевой экран сетевого уровня обнаруживать специальные атаки на веб-системы, такие как XSS, SQL injection и прочие?

Выберите один ответ:

- a. Да
- b. Нет

Межсетевой экран обычно умеет смотреть только стандартные заголовки сетевого уровня (IP адрес, порт, сетевой протокол) и по ним фильтровать. Он не заглядывает внутрь пакетов более высокого уровня (таких, как http).

Вопрос 13

Выполнен

Баллов: 1,00 из 1,00

29. Какие уязвимости относятся к классу угроз OWASP Top 10 A08 Software and Data Integrity Failures? Выберите все верные варианты.

Выберите один или несколько ответов:

- a. CSRF (cross site request forgery)
- b. Не использование многофакторной аутентификации
- c. Загрузка сторонних библиотек из ненадежных источников
- d. Хранение паролей в открытом виде
- e. Инъекция в командную строку
- f. Использование простых паролей
- g. Отсутствие проверок целостности в цепочках CI/CD
- h. Отсутствие проверки целостности компонентов после загрузки
- i. Установка неиспользуемых библиотек и компонентов
- j. Межсайтовая подделка запросов

К данному классу угроз относятся все угрозы, связанные с загрузкой или обновлением приложений или библиотек без проверки целостности того, что именно загружается. В случае использования автоматизированной установки, проверка должна быть встроена в автоматическую цепочку.

Вопрос 14

Выполнен

Баллов: 1,00 из 1,00

К какой из угроз OWASP Top 10 относится использование предсказуемого генератора случайных чисел? Выберите правильный вариант.

Выберите один ответ:

- a. A03 Injection
- b. A04 Insecure Design
- c. A02 Cryptographic Failures
- d. A01 Broken Access Control
- e. A05 Security Misconfiguration

Такого рода уязвимости относятся к неправильному использованию криптографических механизмов. В данном случае даже использование генератора случайных чисел (например, для создания паролей и ключей) не гарантирует безопасность, если выбран небезопасный (не криптографически стойкий, предсказуемый) алгоритм генерации.

Вопрос 15

Выполнен

Баллов: 1,00 из 1,00

Как называется наиболее известный рейтинг 10 наиболее актуальных угроз для веб-приложений? Напишите название на английском.

Ответ: OWASP Top 10

Вопрос 16

Выполнен

Баллов: 1,00 из 1,00

Вы анализируете приложение и видите, что при смене пароля от пользователя не требуется указать текущий пароль. Т.е. пользователь может поменять пароль, указывая свой логин и дважды – новый пароль в системе. При этом система не проверяет старый пароль пользователя, т.е. не просит для подтверждения указать старый пароль. Подумайте, безопасна ли такая схема. К какой из угроз OWASP Top 10 вы бы отнесли данную уязвимость в системе? Выберите один ответ.

Выберите один ответ:

- a. A02 Cryptographic Failures
- b. A04 Insecure Design
- c. A03 Injection
- d. A05 Security Misconfiguration
- e. A08 Software and Data Integrity Failures

Такого рода уязвимость – недостаточная защита идентификационных данных пользователя (CWE-522), т.к. злоумышленник легко может поменять пароль пользователя, ненадолго получив доступ к устройству (или вообще обойдя механизмы проверки). При этом такая ненадежная проверка была заложена при проектировании системы, т.е. это Insecure Design.

Вопрос 17

Выполнен

Баллов: 1,00 из 1,00

Вы обнаружили, что при сборке программы зафиксированы конкретные версии сторонних библиотек, при этом не используется сканирование на безопасность внешних уязвимостей (SCA, software composition analisys), а так же не определена политика обновления пакетов. К каким возможным рискам (в терминологии owap top 10) это может привести (наиболее близкий вариант, выберете один)

- a. A03:2021 – Injection
- b. A07:2021 – Identification and Authentication Failures
- c. A06:2021 – Vulnerable and Outdated Components
- d. A02:2021 – Cryptographic Failures
- e. A08:2021 – Software and Data Integrity Failures

Вопрос 18

Выполнен

Баллов: 1,00 из 1,00

К какой из угроз OWASP Top 10 относится уязвимость в системе, при которой не отловленные исключения (отладочная информация об ошибках) отображаются пользователю системы? Выберите правильный вариант ответа.

Выберите один ответ:

- a. A05 Security Misconfiguration
- b. A08 Software and Data Integrity Failures
- c. A04 Insecure Design
- d. A01 Broken Access Control
- e. A03 Injection
- f. A02 Cryptographic Failures

Отображение отладочной информации пользователю предоставляет злоумышленнику много материала для анализа и дальнейшего взлома системы. Это просто небезопасная настройка.

Вопрос 19

Выполнен

Баллов: 1,00 из 1,00

Как называются уязвимости, при которых злоумышленник получает возможность внедрить свою информацию (пользовательский ввод) в запрос к сторонней системе, что приводит к модификации исходного запроса? Выберите правильный вариант.

Выберите один ответ:

- a. Ошибки криптографии
- b. Нарушения контроля доступа
- c. Ошибки идентификации и аутентификации
- d. Инъекции
- e. Security Misconfiguration

Вопрос 20

Выполнен

Баллов: 1,00 из 1,00

К какой из угроз OWASP Top 10 относится уязвимость в системе, при которой папка с кодами программы открыта на запись и добавление файлов для пользователя операционной системы, с правами которого запускается веб-сервер? Выберите правильный вариант ответа.

Выберите один ответ:

- a. A05 Security Misconfiguration
- b. A03 Injection
- c. A04 Insecure Design
- d. A08 Software and Data Integrity Failures
- e. A01 Broken Access Control
- f. A02 Cryptographic Failures

Вопрос 21

Выполнен

Баллов: 1,00 из 1,00

Вы анализируете приложение и видите, что в нем используется большое количество сторонних библиотек. При этом, при установке библиотек и приложений не осуществляется контроль целостности, а сами библиотеки загружаются из неизвестных репозиториев. К какой из угроз OWASP Top 10 относится подобная уязвимость? Выберите правильный вариант ответа.

Выберите один ответ:

- a. A08 Software and Data Integrity Failures
- b. A02 Cryptographic Failures
- c. A07 Identification and Authentication Failures
- d. A01 Broken Access Control
- e. A05 Security Misconfiguration
- f. A06 Vulnerable And Outdated Components
- g. A03 Injection

При установке библиотек обязательно необходимо проверять контроль целостности исходных кодов или исполняемых файлов (проверка подписи, контрольных сумм и т.п.). Вообще, рекомендуется загружать приложения и обновления из корпоративного репозитория (где лежат только библиотеки, уже прошедшие проверку на безопасность).

Вопрос 22

Выполнен

Баллов: 1,00 из 1,00

Вы обнаружили в операционной системе библиотеку, которая принимает и обрабатывает сетевые запросы. При этом, для работы вашего приложения, данная библиотека не используется. Подумайте, почему так делать не стоит. К какой из угроз OWASP Top 10 вы бы отнесли подобную уязвимость? Выберите правильный вариант ответа.

Выберите один ответ:

- a. A02 Cryptographic Failures
- b. A08 Software and Data Integrity Failures
- c. A03 Injection
- d. A01 Broken Access Control
- e. A04 Insecure Design
- f. A05 Security Misconfiguration

Установка ненужных сервисов увеличивает поверхность атаки для злоумышленника – это ошибки небезопасной конфигурации (настройки).

Вопрос 23

Выполнен

Баллов: 1,00 из 1,00

Какому классу угроз OWASP Top 10 противостоят автоматизированные средства сканирования уязвимых зависимостей? Выберите правильный ответ.

Выберите один ответ:

- a. A01 Broken Access Control
- b. A06 Vulnerable and outdated components
- c. (выбор из списка)
- d. A08 Software and Data Integrity Failures
- e. A03 Injection
- f. A04 Insecure Design
- g. A05 Security Misconfiguration

Вопрос 24

Выполнен

Баллов: 1,00 из 1,00

В протоколе HTTP есть специальные заголовки, которые повышают безопасность работы системы. Однако часто они просто не используются разработчиками, в результате чего система остается менее защищенной. К какой из угроз OWASP Top 10 вы бы отнесли подобную уязвимость? Выберите правильный вариант ответа.

Выберите один ответ:

- a. A01 Broken Access Control
- b. A08 Software and Data Integrity Failures
- c. A02 Cryptographic Failures
- d. A05 Security Misconfiguration
- e. A03 Injection
- f. A04 Insecure Design

Не использование или некорректное использование имеющихся механизмов безопасности – это ошибки небезопасной конфигурации (настройки).

Вопрос 25

Выполнен

Баллов: 1,00 из 1,00

К какой из угроз OWASP Top 10 относится уязвимость в системе, при которой пароли от учетных записей пользователей хранятся в базе данных в открытом (незашифрованном и не хешированном) виде? Выберите правильный вариант ответа.

Выберите один ответ:

- a. A03 Injection
- b. A05 Security Misconfiguration
- c. A08 Software and Data Integrity Failures
- d. A01 Broken Access Control
- e. A04 Insecure Design
- f. A02 Cryptographic Failures

Вопрос 26

Выполнен

Баллов: 1,00 из 1,00

Является ли безопасной передача чувствительной информации по протоколу http?

Выберите один ответ:

- a. Нет
- b. Да

Чувствительную информацию можно передавать только по зашифрованному каналу (используйте https).

Вопрос 27

Выполнен

Баллов: 1,00 из 1,00

К какой из угроз OWASP Top 10 относится уязвимость SQL инъекции? Выберите правильный вариант.

Выберите один ответ:

- a. A02 Cryptographic Failures
- b. A01 Broken Access Control
- c. A03 Injection
- d. A04 Insecure Design
- e. A05 Security Misconfiguration

Вопрос 28

Выполнен

Баллов: 1,00 из 1,00

Какая политика должна использоваться по умолчанию при настройке прав доступа?

Выберите один ответ:

- a. Запрещено все, что не разрешено
- b. Разрешено все, что не запрещено

Вопрос 29

Выполнен

Баллов: 1,00 из 1,00

Какие уязвимости относятся к классу угроз OWASP Top 10 A07 Identification and Authentication Failures? Выберите все верные варианты.

Выберите один или несколько ответов:

- a. Установка неиспользуемых библиотек и компонентов
- b. Использование небезопасных библиотек
- c. Межсайтовая подделка запросов
- d. Инъекция в командную строку
- e. Хранение паролей в открытом виде
- f. CSRF (cross site request forgery)
- g. Передача идентификатора сессии в GET параметрах запроса
- h. Использование простых паролей
- i. Не использование многофакторной аутентификации

К данному классу угроз относятся все угрозы, связанные с нарушением механизмов аутентификации (в том числе, связанные с хранением и передачей паролей и идентификаторов сессии).

Вопрос 30

Выполнен

Баллов: 1,00 из 1,00

К какой из угроз OWASP Top 10 относится уязвимость CSRF? Выберите правильный вариант.

Выберите один ответ:

- a. A01 Broken Access Control
- b. A03 Injection
- c. A05 Security Misconfiguration
- d. A04 Insecure Design
- e. A02 Cryptographic Failures

Атака межсайтовой подделки запросов относится к классу атак через нарушения контроля доступа.

Служба поддержки сайта

Вы зашли под именем Новиков Виталий Сергеевич (Выход)