Задача: Исправление уязвимости CVE-2021-41773 на web сервере

**Описание уязвимости:**

CVE-2021-41773 - это уязвимость в Apache HTTP Server, которая позволяет злоумышленникам выполнить произвольный код на сервере. Уязвимость возникает из-за неправильной обработки запросов в модуле mod\_cgi.

**Шаги для исправления уязвимости:**

1. **Обновление Apache HTTP Server:**

* Обновите Apache HTTP Server до последней версии, в которой исправлена уязвимость (например, Apache HTTP Server 2.4.51 или новее).
* Убедитесь, что все зависимости и модули также обновлены до последней версии.

1. **Установка патча:**

* Если обновление Apache HTTP Server не возможно, установите патч, который исправляет уязвимость.
* Патч можно скачать с официального сайта Apache или из репозитория дистрибутива Linux.

1. **Конфигурация mod\_cgi:**

* Проверьте конфигурацию модуля mod\_cgi и убедитесь, что он правильно настроен.
* Убедитесь, что директива Options установлена в значение -ExecCGI, чтобы предотвратить выполнение CGI-скриптов в директориях, где они не нужны.

1. **Проверка конфигурации:**

* Проверьте конфигурацию Apache HTTP Server и убедитесь, что все изменения были приименены правильно.
* Убедитесь, что сервер работает корректно и не выдает ошибок.

1. **Тестирование:**

* Протестируйте сервер, чтобы убедиться, что уязвимость исправлена.
* Используйте инструменты, такие как curl или wget, чтобы проверить, что сервер правильно обрабатывает запросы.

**Контрольные вопросы:**

* Была ли обновлена версия Apache HTTP Server?
* Был ли установлен патч для исправления уязвимости?
* Была ли проверена конфигурация модуля mod\_cgi?
* Была ли проверена конфигурация Apache HTTP Server?
* Было ли проведено тестирование сервера?

**Результаты:**

* Уязвимость CVE-2021-41773 исправлена.
* Сервер работает корректно и не выдает ошибок.
* Конфигурация Apache HTTP Server проверена и исправлена.

**Время выполнения:**

* Ожидаемое время выполнения: 30 минут.
* Максимальное время выполнения: 1 час.

**Примечания:**

* Убедитесь, что все изменения были применены правильно и не повлияли на работу сервера.
* Если у вас возникли проблемы при исправлении уязвимости, обратитесь к специалисту SOC L2 или L3 для дальнейшей помощи.