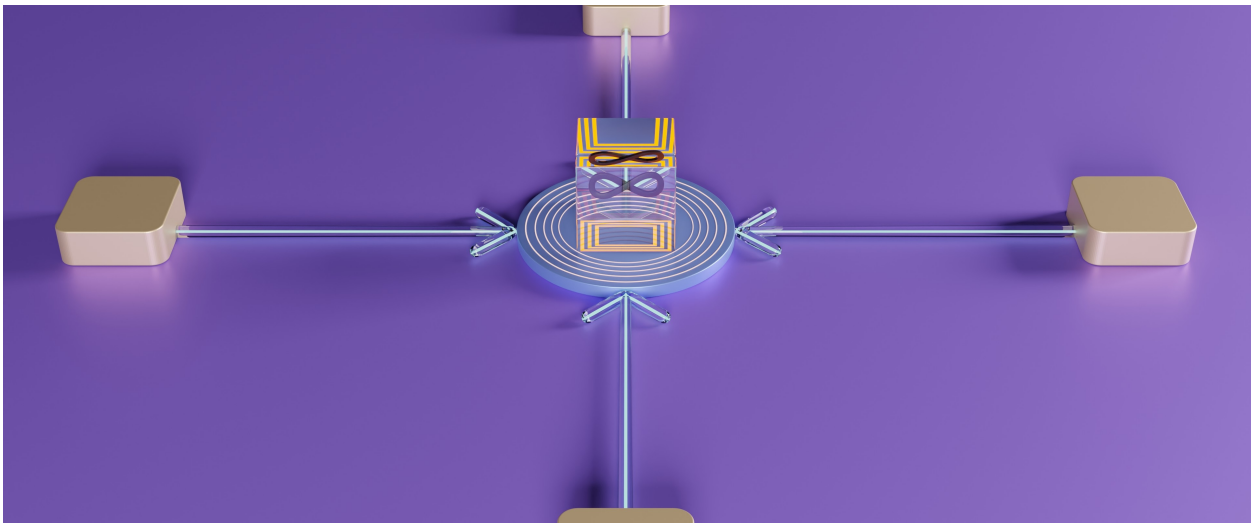

DevSecOps 2023

Задание

В центре внимания — веб-приложение, написанное на Python Flask “*dilettantish-internal-portal*”. По легенде, небольшая компания наняла подрядчика, который оказался не особо осведомленным в вопросах информационной безопасности *(руководство не захотело выделять больше денег на разработку, тем самым выбор пал на подрядчика по низу рынка)*.

Приложение обладает следующим функционалом и ограничениями:

- Администратор может создавать пользователей и редактировать список должностей внутри компании;
- Пользователь не может редактировать свой профиль (кроме как сменить фотографию профиля);
- Профили служат для того, чтобы сотрудники могли смотреть карточки друг друга (номера телефонов, адреса ЭП, должность). Информация, расположенная в карточке, только для ***авторизованного*** пользователя;
- Пользователи могут создавать страницы в *Базе знаний* (как в блоге), чтобы обмениваться инструкциями по работе. Функционал не ограничивает пользователя в возможности модифицировать страницу так, как ему нужно;

- Главная страница приложения служит визитной карточкой компании. *Будет жалко, если кто-нибудь дефейснит лендинг вашей компании.*

Да, приложение выглядит “суховато”, но ничего не говорите руководству, а то они заставят вас дорабатывать не только безопасность, но и функционал (за доширак).

Ваши глобальные задачи:

- Наладить процесс разработки в команде (необходимо развернуть систему контроля версий. Обратите внимание на другие части задания — от этого может зависеть выбор продукта. Система контроля версий должна быть доступна внутри VPN сети по адресу git.team-domain.devsecops. Репозитории могут быть приватными на время соревнования, но необходимо предусмотреть учетную запись для организаторов);
- Найти и исправить проблемы в безопасности веб-приложения;
- Реализовать тесты приложения (здесь достаточно простого теста, просто чтобы он был);
- Реализовать процесс автоматического развертывания веб-приложения, с автоматическим тестированием (подобно тому, как работает Github Actions);
- Желательно наличие двух непересекающихся контуров: Dev и Prod;
- Найти и проэксплуатировать проблемы безопасности веб-приложений команд-соперников;
- *А также, не забудьте придумать легенду вашей компании и красиво оформить главную страничку).*

Вам будут выданы конфиги VPN (wireguard) (в свете того, что Timeweb.cloud предоставляют инфраструктуру, конфиги нужны только для доменов), один/несколько конфигов для вашего сервера/серверов, а другие для участников команды.

На настройку инфраструктуры вам отводится 2 дня (10 и 11 апреля), после чего необходимо опубликовать наружу ваш веб-сервис — для этого необходимо

забиндить адрес вашего сервиса в доменной DNS зоне *.devsecops (написать в чате, на какой домен необходимо создать A и PTR записи).

После того, как ваш сервис публично (в рамках VPN сети) опубликован, вы можете продолжать работы по разработке и администрированию, а также можете начинать работы по пентесту сервисов других команд.

В опубликованном приложении необходимо выполнить ряд действий:

- Создать не менее 5 пользователей с разными должностями (используйте *нормальные* ФИО и другие данные, похожие на настоящие. Слив этих данных будет засчитываться взломавшей вас команде);
- Создать пользователя с ролью user, username — vulnuser, пароль — vulnuser (эта учетная запись будет выполнять роль взломанного/недобросовестного пользователя);

Соревнование оценивается одновременно по трем направлениям:

- Исправление проблем безопасности;
- Системное администрирование;
- Пентест.

Отчетность по заданиям в следующей форме:

- https://forms.gle/mVKc2qLiHvaj7hq1A — форма для сдачи найденных уязвимостей и их исправлений;
- По системному администрированию, необходимо создать репозиторий, содержащий набор необходимых скриптов и др. файлов для выполнения задания. В репозитории должен быть файл README.md, содержащий описание вашей инфраструктуры и инструкции по работе с ней (вы можете сделать этот репозиторий приватным и создать организаторскую учетную запись).

- По пентесту необходимо создать репозиторий с райтапами для каждой найденной уязвимости для каждой команды.

13 апреля будет проходить презентация результатов соревнования каждой команды. Необходимо предоставить доклад со слайдами (~7 минут), отражающий все 3 аспекта соревнования и являющийся компиляцией всех отчётов.

P.S. Начиная с 12 апреля, 12:00 ваше веб-приложение должно быть доступно каждому в VPN сети. При проведении тестирования на проникновение, запрещается выполнять действия, приводящие к непоправимым последствием (например, нельзя стереть весь репозиторий с кодом, нельзя ломать логику работы приложения, но можно дефейсить главную страницу. Если не знаете, можно ли сделать то или иное действие, лучше спросите сначала организаторов). Если существует несколько способов (подходов, разных уязвимостей. Например, несмотря на то, что есть специально созданный уязвимый пользователь, если вы найдете способ попасть в систему, не используя его, опишите этот способ) сделать в системе одно и то же, опишите все, какие найдете.

Удачи!