Задание по дисциплине

Дисциплина	Разработка защищённых программных систем
Тема	Задание по теме 6 «Средства защиты приложений»
Форма проверки	**Домашнее задание проверяется преподавателем**
Имя преподавателя	Владимир Телепов
Время выполнения	1,5–2 часа
Цель задания	Научиться использовать средства анализа безопасности приложений — SAST и DAST
Инструменты для выполнения ДЗ	Для выполнения задания используйте Google Документы и виртуальную машину из прошлых домашних работ
Правила приема работы	1. Для выполнения задания создайте Google Документ и заполняйте информацию по этапам в нём. 2. Прикрепите ссылку на Google Документ. Важно: убедитесь в том, что по ссылке есть доступ. Название файла должно содержать фамилию и имя студента, номер ДЗ (ДЗ по Теме 6)
Критерии оценки	**Задание считается выполненным:** - прикреплена ссылка на файл с выполненным заданием, - доступы к материалам открыты, - выполнены все остальные требования чеклиста самопроверки. **Задание не выполнено:** - файл с заданием не прикреплён или отсутствует доступ по ссылке, - не выполнены все остальные требования чеклиста самопроверки
Дедлайн	*Срок сдачи — семь рабочих дней после окончания прослушивания вебинара*

Инструкция по выполнению домашнего задания

Этап 0

Изучите информацию лекции и вебинара по теме 6.

Этап 1

К созданной в теме 5 инфраструктуре добавьте компонент OWASP ZAP:

1. Установите JDK командой apt install default-jdk.
2. Установите DAST-инструмент OWASP ZAP. Для этого загрузите установочный файл по ссылке, и запустите его.
3. Выполните установку OWASP ZAP и запустите приложение. При необходимости, подождите пару минут, пока оно обновится, и перезапустите его.

Этап 2

Установите инструмент для статического анализа Python кода Bandit.

Для этого выполните действия:

1. Установите менеджер Python-пакетов pip (sudo apt install python3-pip).
2. Установите сканер кода Bandit (pip3 install bandit).

Этап 3

Выполните статическое сканирование исходного кода приложения PyGoat* с помощью Bandit. Для этого запустите терминал в директории с PyGoat (PyGoat-master) и выполните команду bandit -r . -ll.

* Архив с репозиторием приложения Pygoat доступен по ссылке.

Этап 4

1. Запустите контейнер с приложением PyGoat и опубликуйте его на порту 8000 (docker run -it -p 8000:8000 *имя_образа_pygoat*).
2. Запустите сканер OWASP ZAP, выберите Automated Scan и в поле URL to attack введите http://127.0.0.1:8000.
3. Нажмите Attack и дождитесь завершения сканирования.

Этап 5

В Google Документы загрузите отчёт в свободной форме о найденных уязвимостях в приложении PyGoat.

Чеклист самопроверки

Критерии выполнения задания	Отметка о выполнении
Составлен отчёт о сканировании Предоставлены отчёты в следующих форматах: – Отчёт по DAST (1 балл) – Отчёт по SAST (1 балл) – Предоставлены выводы про дополнительным исследованиям кода и приложения (1 балл)	3
Выполнено сканирование DAST (предоставлены скриншоты в отчёте)	2
Выполнено сканирование SAST (предоставлены скриншоты в отчёте)	2
Предложены новые выводы, рекомендации по улучшения задания	3