

Задание по дисциплине

Дисциплина	Разработка защищенных программных систем
Тема	Задание по теме 13
Форма проверки	Домашнее задание с самопроверкой <i>Совет: выполняйте домашнее задание сразу после изучения темы</i>
Имя преподавателя	Владимир Телепов
Время выполнения	80 минут
Цель задания	Получить навыки обратной разработки уже известных уязвимостей
Инструменты для выполнения ДЗ	Для выполнения задания используйте Google Docs / Яндекс документы
Правила приема работы	1. Для выполнения задания создайте Google Doc / Яндекс документ и заполняйте информацию по этапам в нём 2. Прикрепите ссылку на Google Doc / Яндекс документ. Важно: убедитесь в том, что по ссылке есть доступ. Название файла должно содержать фамилию и имя студента и номер ДЗ (ДЗ по Теме 13)
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 прикреплен или отсутствует доступ по ссылке - не выполнены все остальные требования чеклиста самопроверки
Дедлайн	<i>Срок сдачи 7 рабочих дней после окончания прослушивания вебинара</i>

Этап 0

Изучите информацию вебинара по теме 13.

Этап 1

Выберите произвольную уязвимость из каталога CVE, удовлетворяющую следующим требованиям:

1. Оценка по шкале CVSS: не ниже 7.0
2. Уязвимость найдена в веб-приложении или библиотеке, код которых открыт и доступен по публичной ссылке.
3. Уязвимость имеет статус исправленной.

Этап 2

Соберите имеющуюся информацию об уязвимости и проанализируйте её.

Этап 3

Оформите документ с разбором уязвимости, в формате, структурно аналогичном статье <https://habr.com/ru/company/pt/blog/694720/>.

Этап 4

Разместите ссылку на документ в Google Doc / Яндекс документ. Проверьте доступ к документу. Название файла должно содержать фамилию, имя студента и номер ДЗ (ДЗ по Теме 13).

Чек-лист самопроверки

Критерии выполнения задания	Отметка о выполнении
Выполнены все этапы задания	●
Итоговый отчёт содержит информацию об полном жизненном цикле уязвимости (как появилась, как была обнаружена, как была исправлена)	●
Осуществлен детальный разбор уязвимости в исходном коде приложения или библиотеке и предложенного вендором патча	●
Даны рекомендации по тестированию собственных проектов на аналогичные типы уязвимостей	●

Даны рекомендации по закрытию атак на данную уязвимость на сетевом периметре	•
--	---