Invicti

План интеграции автоматического аудита безопасности веб-приложений на базе Acunetix в процессы DevSecOps

- что происходит?
- как подружить Dev и Sec
- автоматизация

Какие последствия могут быть у взлома веб-приложения?

- Получение доступа к сети
- Кража данных клиентов
- Потеря денег
- Удар по репутации
- Юридические риски
- Злорадство конкурентов
- Атака на ваших клиентов
- … и так далее

Почему уязвимы веб-приложения

- ~~У кого-то руки из ж~~
- Устаревшие или непроверенные технологии
- Ошибки в коде
- Халатность при разработке веб-приложений
- Отсутствие «полной картины» для анализа защищенности
- Отсутствие инвентаризации и контроля веб-приложений
- Недостаточные знания разработчиков в области ИБ

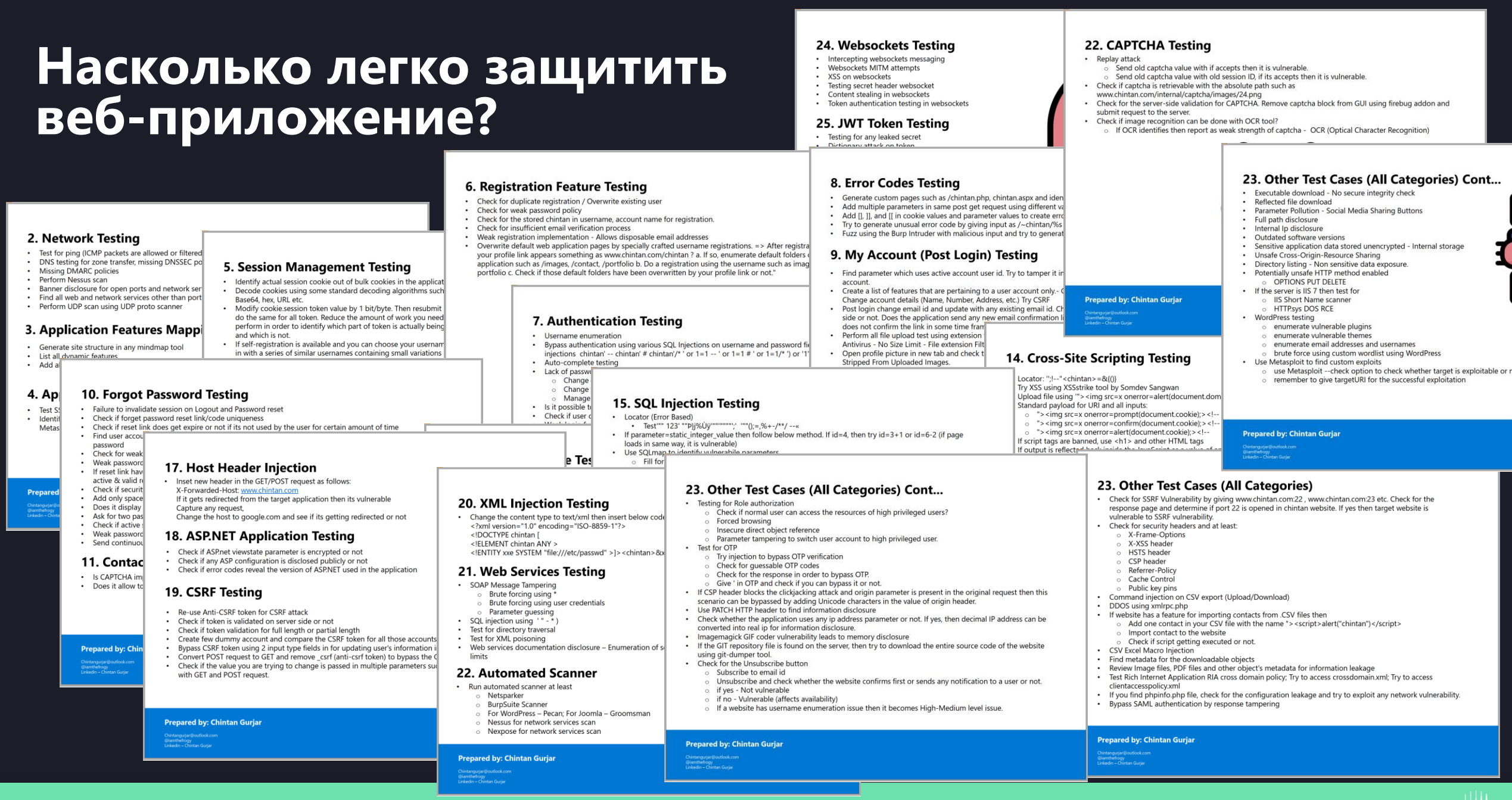
Почему нельзя сделать сразу хорошо?

Программисты допускают ошибки так же часто, как люди в письмах.
Только текст их «писем» состоит из десятков миллионов символов.

Чтобы разрабатывать безопасно, нужно

- Знать, что так можно
- Знать, с помощью чего так можно
- Выбрать и настроить
- Успеть сделать до того, как «клюнет»

Насколько легко защитить веб-приложение?



Invicti

Насколько легко защитить веб-сайт?

https://www.acunetix.com/vulnerabilities/web/

Более 6.000 **видов** уязвимостей!

Вчера было лучше?

Нет:

- **люди были так же невнимательны**
- **уязвимости точно так же удивляли**
- **подрядчики делали в стиле «и так сойдет»**
- **качество кода не зависело от размеров компании**

Что поменялось?

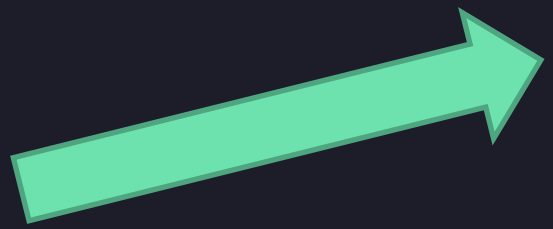
Больше нет «security by practical obscurity»

Каждый «школьник» может скачать сканер и захватить любой веб-сайт ради интереса.

Миллионы взломанных серверов постоянно сканируют веб-сайты на наличие уязвимостей.

Установка вредоносного кода - автоматически.

Ломают всех.
И вас взломают просто так
поделятся ссылкой в телеграме,
а толпа сочувствующих добьет ваш сервер



Что делать?

- Нельзя делать «Security» в одно лицо
- «Security» должен стать обязательной частью процесса
- DevOps ускоряет процесс разработки всего лишь на 8-10%
  Нельзя, чтобы Sec его тормозил
- Использовать удобные автоматизированные средства
- Забыть про «команду» и «все мы в одной лодке»
  Процесс должен быть прозрачен и регламентирован
- Никаких процессов ради процессов – решения принимаются разумно и от рисков
- Готовьте план и закрывайте максимум задач минимальными изменениями

Что делать v2.0 или «Как же мы ошибались»

- Разработчики и безопасники должны хоть раз лично встретиться
- Вести список конфигов, секретов, сертификатов и учетных записей
- Вести карту соответствия объектов/ресурсов (ассетов) и ответственных
- Простая понятная схема деплоя/SDLC должна быть доступна всем вовлеченным
- Вести инвентаризацию и журнал изменений и делиться журналом в обе стороны
- Обсуждать требования от целей
- Изучить и здраво (а не стереотипно) оценивать
  линтеры, SAST-ы и DAST-ы – не покупать из-за моды, а прийти органическим путем
- Не бояться пускать «на кухню» сторонних специалистов со свежим взглядом
- Следить за белыми пятнами в знаниях разработчиков, админов, DevOps-ов и Sec-ов

Уязвимость найдена и назначена ответственной группе разработчиков

Разработчики исправляют уязвимость

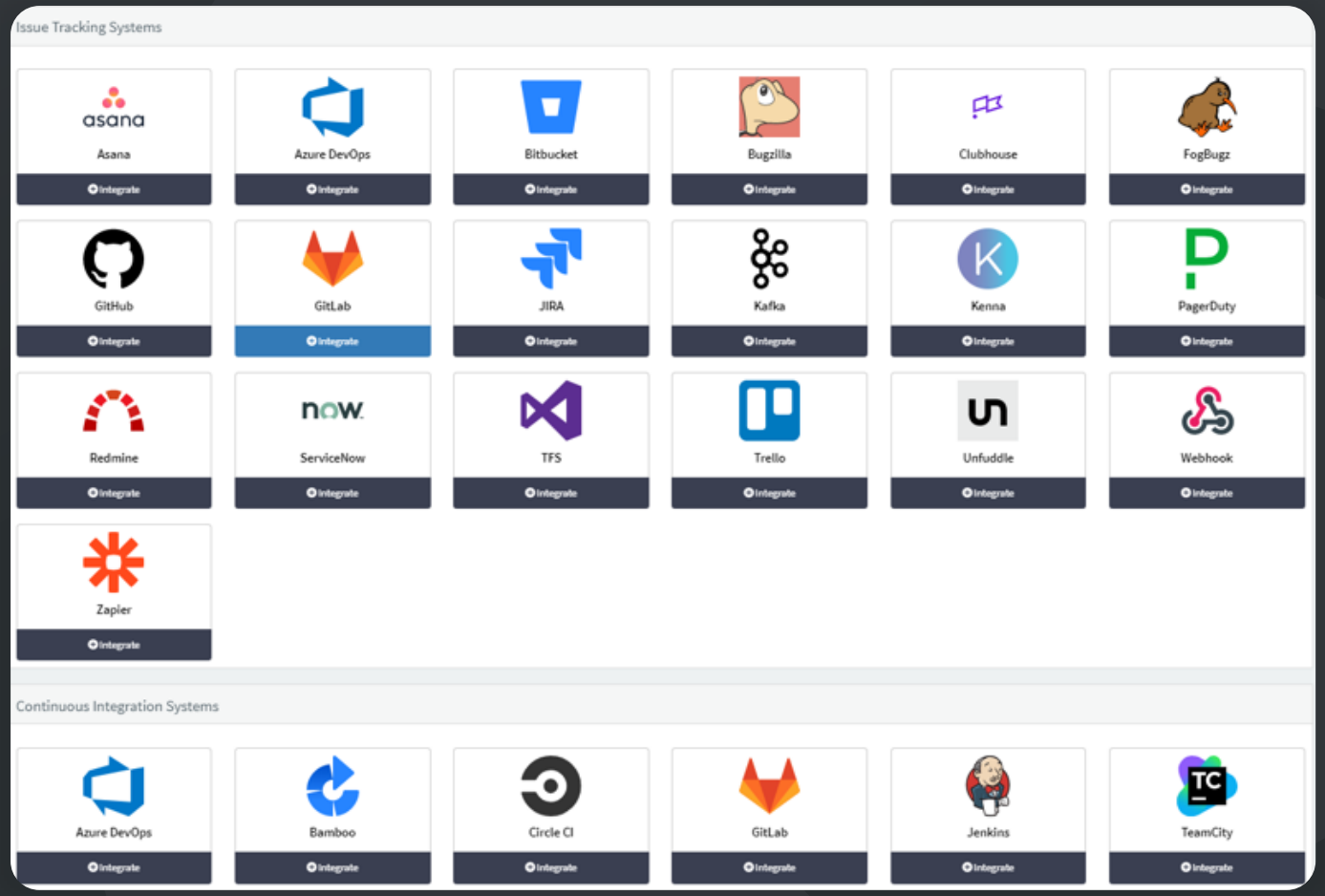
Acunetix проверяет, что проблема исправлена

Если уязвимость еще есть, задача исправить ставится заново

Если уязвимости нет, задача закрывается, руководитель получает оповещение

Интеграция с инструментами автоматизации безопасной разработки

- Системы трекинга задач
- CI/CD
- API



acunetix

Технология DeepScan

Современные веб-приложения написаны с использованием HTML5 и JavaScript. DeepScan, основанные на Chromium позволяет исследовать такие веб-приложения эффективнее других сканеров.

DeepScan может автоматически распознать популярные фреймворки: Angular, Vue, React и скорректировать стратегию составления структуры веб-приложения.

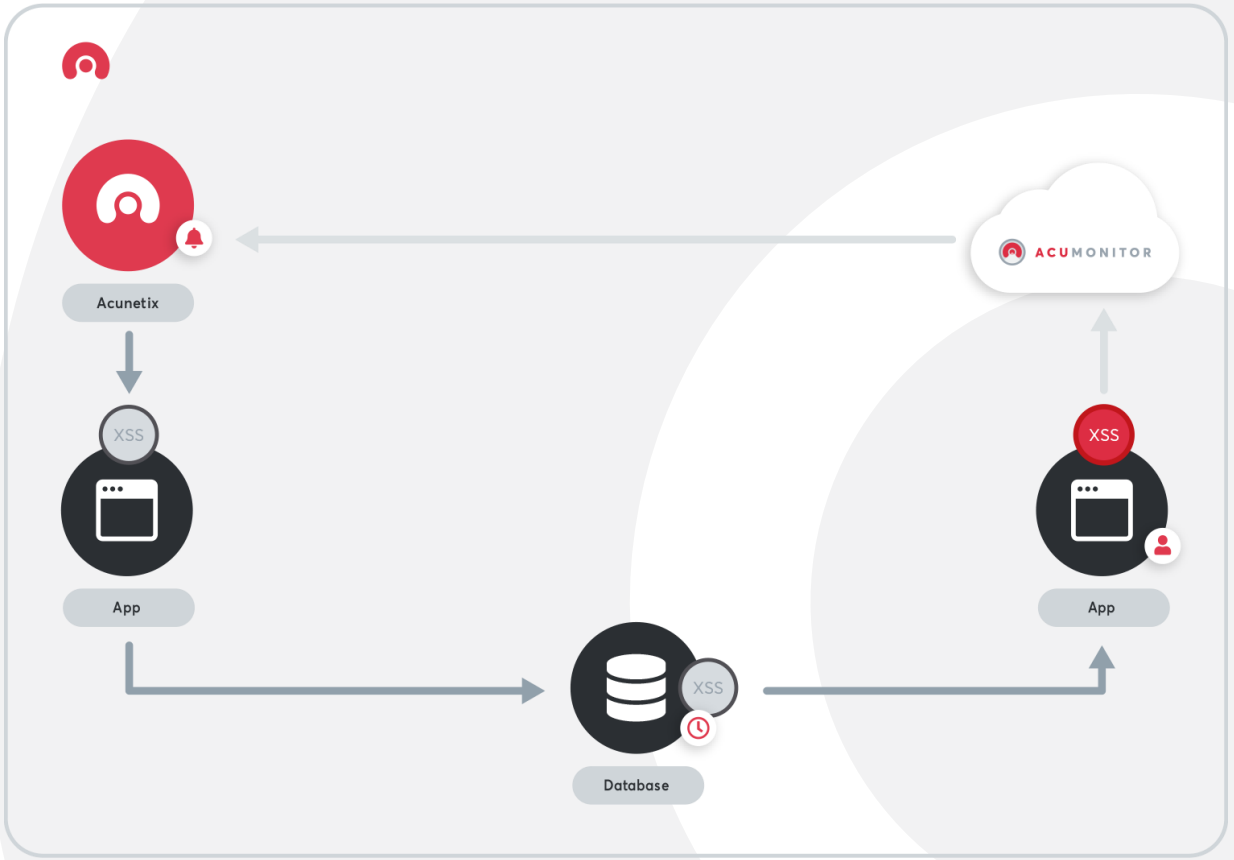
DeepScan может автоматически выполнять вход в закрытые части веб-приложения по паролю, ключам, токенам.

AcuMonitor находит скрытые уязвимости

Acunetix может обнаружить скрытые уязвимости, проверяя реакцию веб-приложения на внешние запросы изнутри.

Таким образом технология AcuMonitor позволяет находить уязвимости, которые не дают о себе знать в ответе от сервера.

AcuMonitor полностью безопасен для веб-приложения и используется, как дополнительный инструмент при сканировании.



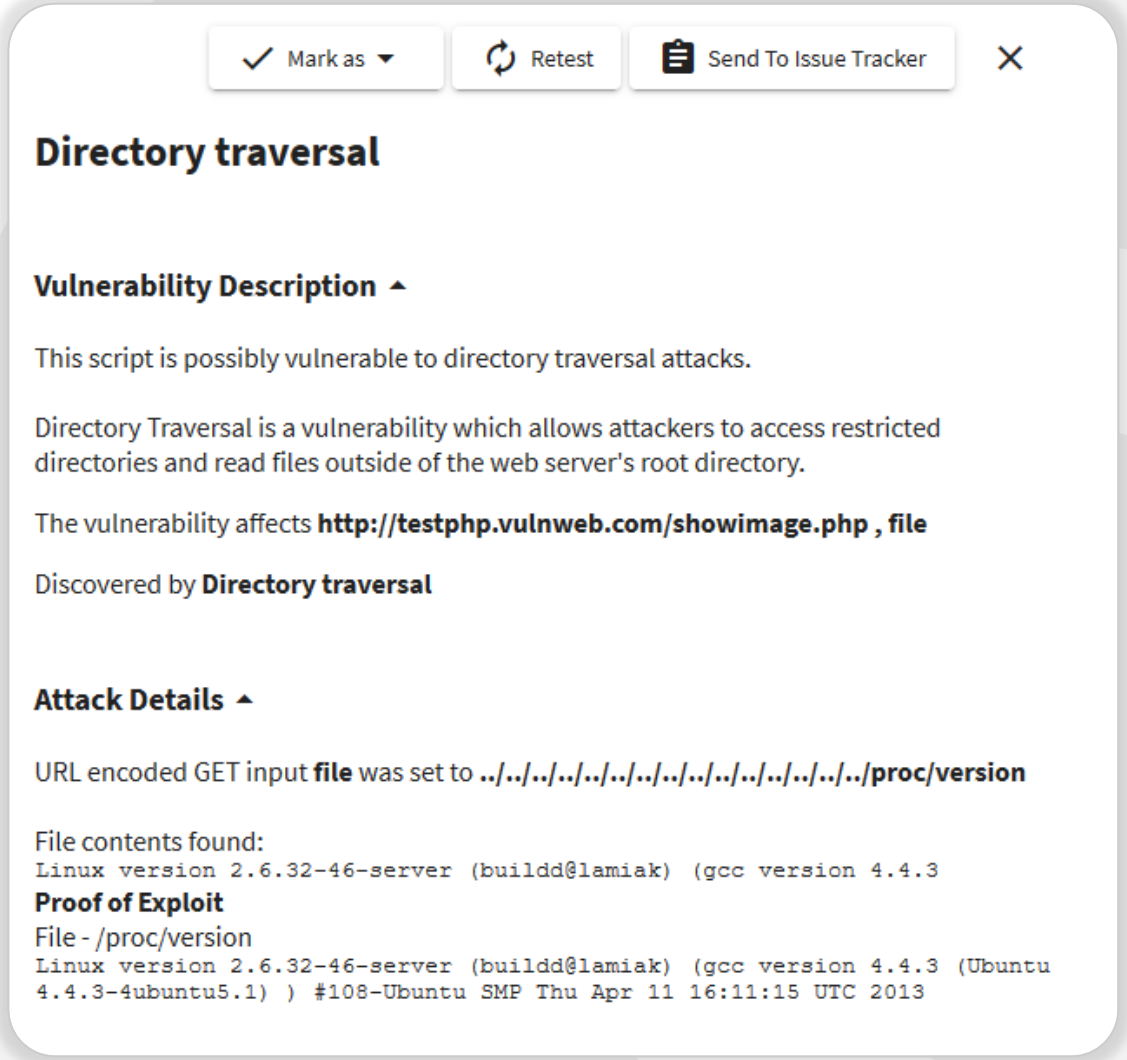
ACUSENSOR обнаруживает

- Создание файлов
- Удаление файлов
- Выполнение кода
- Инъекции заголовков в письма
- Вывод содержимого директорий
- Включение содержимого файлов в исполняемый код

- Изменение файлов
- Загрузку файлов
- Инъекции кода PHP
- Перезапись глобальных переменных
- XSS
- SQL-инъекции
- ...и так далее

Подтверждение уязвимостей

- Acunetix записывает ход своего расследования уязвимости.
- Дополнительно предоставляется подтверждение наличия уязвимости в виде выполненной команды и ответа от сервера.
- Помогает предоставить разработчикам полную картину и ускорить исправление



acunetix

Спасибо!

dm@afi-d.ru
www.Invicti.ru