



DevSecOps в веб-разработке: устранить уязвимости до того, как ими воспользуется хакер

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



Какие последствия могут быть у взлома веб-приложения?

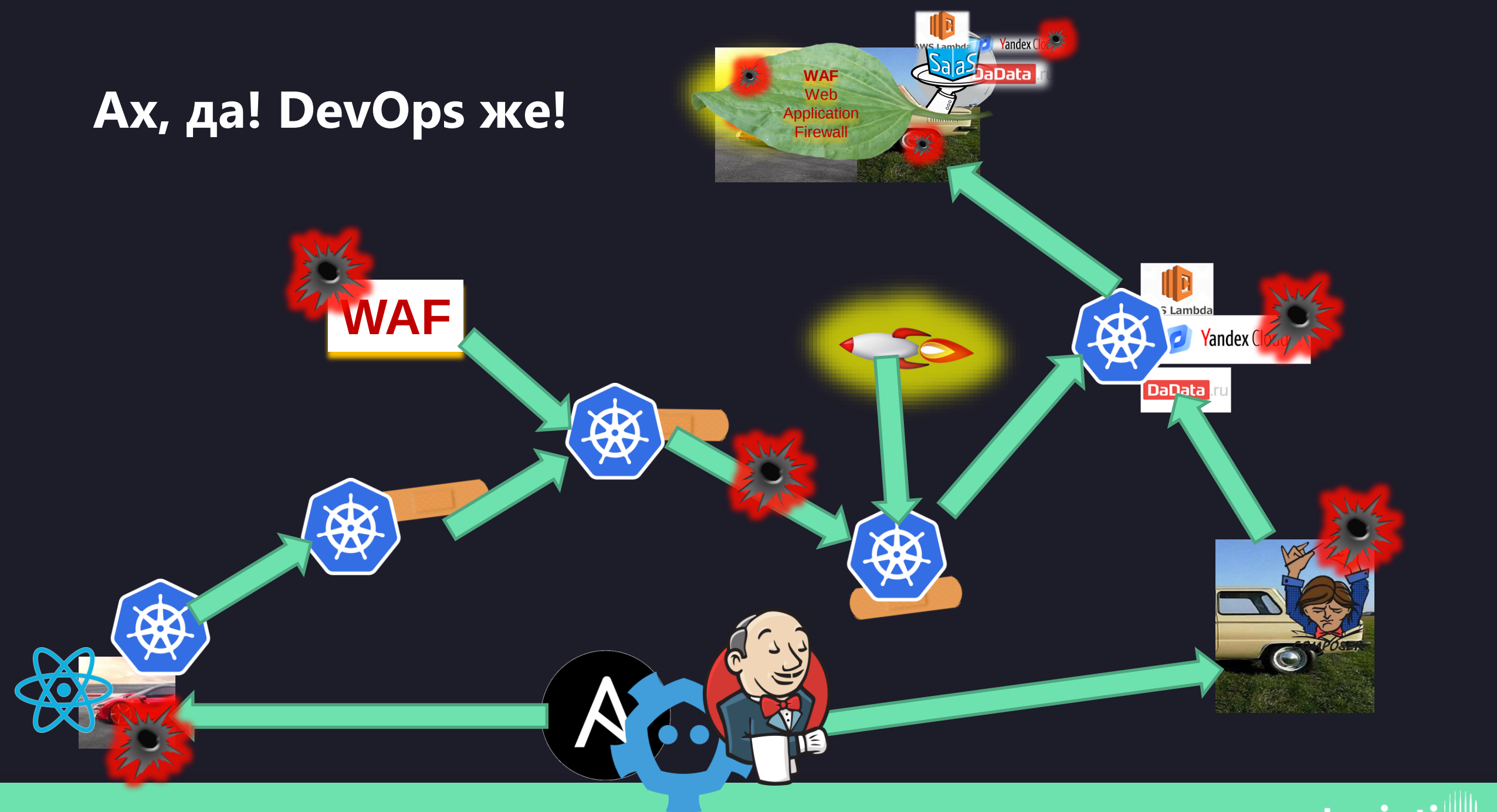
- Получение доступа к сети
- Кража данных клиентов
- Потеря денег
- Удар по репутации
- Юридические риски
- Злорадство конкурентов
- Атака на ваших клиентов
- ... и так далее



Знакомьтесь! Ваше веб-приложение



Ах, да! DevOps же!



Ах, да! Dev **SEC** Ops же!



Почему уязвимы веб-приложения

- 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-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»

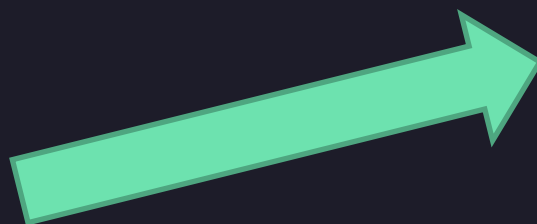
Каждый «школьник» может скачать сканер и захватить любой веб-сайт ради интереса.

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

Установка вредоносного кода - автоматически.

Ломают всех.

И вас взломают просто так
поделится ссылкой в телеграме,
а толпа сочувствующих добьет ваш сервер



SQL InFection

`http://gu[redacted].ru/gp/'&&(select+updatexml(0,concat(0x5c,version()),1))=%27`

Type: Error-based

DBMS: MySQL 5.6.38

318 изменено 8:59

SQL InFection

`http://u[redacted].ru/showimg.php?id_img=0+union+select+1,null,version(),null,null,null,null,8,null,10,11,12,13`

Type: Union-based

DBMS: MariaDB 10.0.10

Shared by: [redacted]

319 15:53

21 апреля

SQL InFection

`https://e[redacted]/newsitem.php?id=cast(version()+as+int)`

Type: Error-based

DBMS: PostgreSQL 8.0.1

Shared by: [redacted]

330 13:31

22 апреля

SQL InFection

`http://g[redacted]u/cart.php?article='+union+select+1,2,3,version(),5,6,7--+`

Type: Union-based

DBMS: MariaDB 10.1.38

Shared by: [redacted]

294 изменено 8:06

SQL InFection

`http://o[redacted]u/common/person.php?num=0+union+select+1,null,null,4,null,null,null,8,9,@@version,11,12,13`

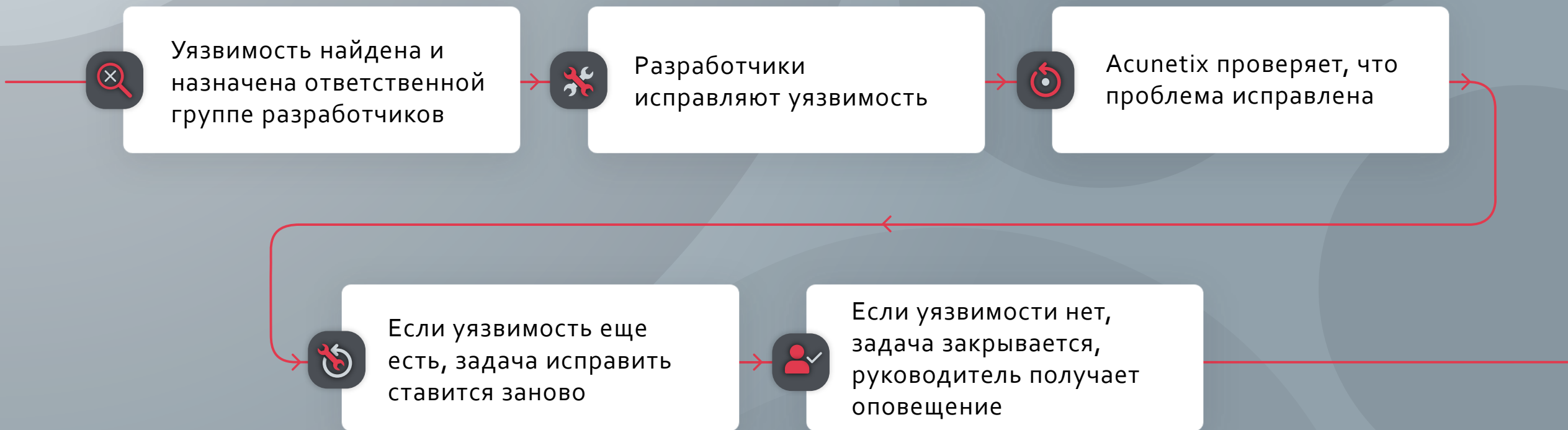
Type: Union-based

Сумасшедший рост задач для специалистов ИБ



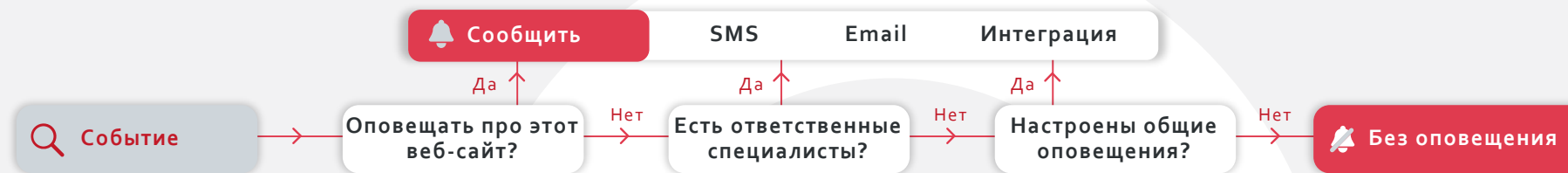
Что делать?

- Нельзя делать «Security» в одно лицо
- «Security» должен стать обязательной частью процесса
- Дружить Dev и Sec
- 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



Настраиваемые процессы оповещения

Клиент может обеспечить удобный мониторинг безопасности 24/7



Test Notification

Clone

Event: Scan Completed

Lowest Severity: Low

Group Scan: ☒

Website: http://test.vulnweb.com

User: Administrator

Test

Update Notification

Clone

Name: Scan Completed

Event: Scan Completed

Group Scan: ☒

Lowest Severity: Information

Scope: Any Website Website Group Website

E-mail Recipients: Person Who Started Scan X

SMS Recipients: Administrator

Excluded Recipients:

Integration Endpoints: Administrator

Save

Notification Priorities

Clone

Event: Scan Completed

Website or Website Group: Low

ORDER	STATUS	NAME	SCOPE
1	Enabled	Scan Completed	Any Website

Save

Интеграция с инструментами автоматизации безопасной разработки



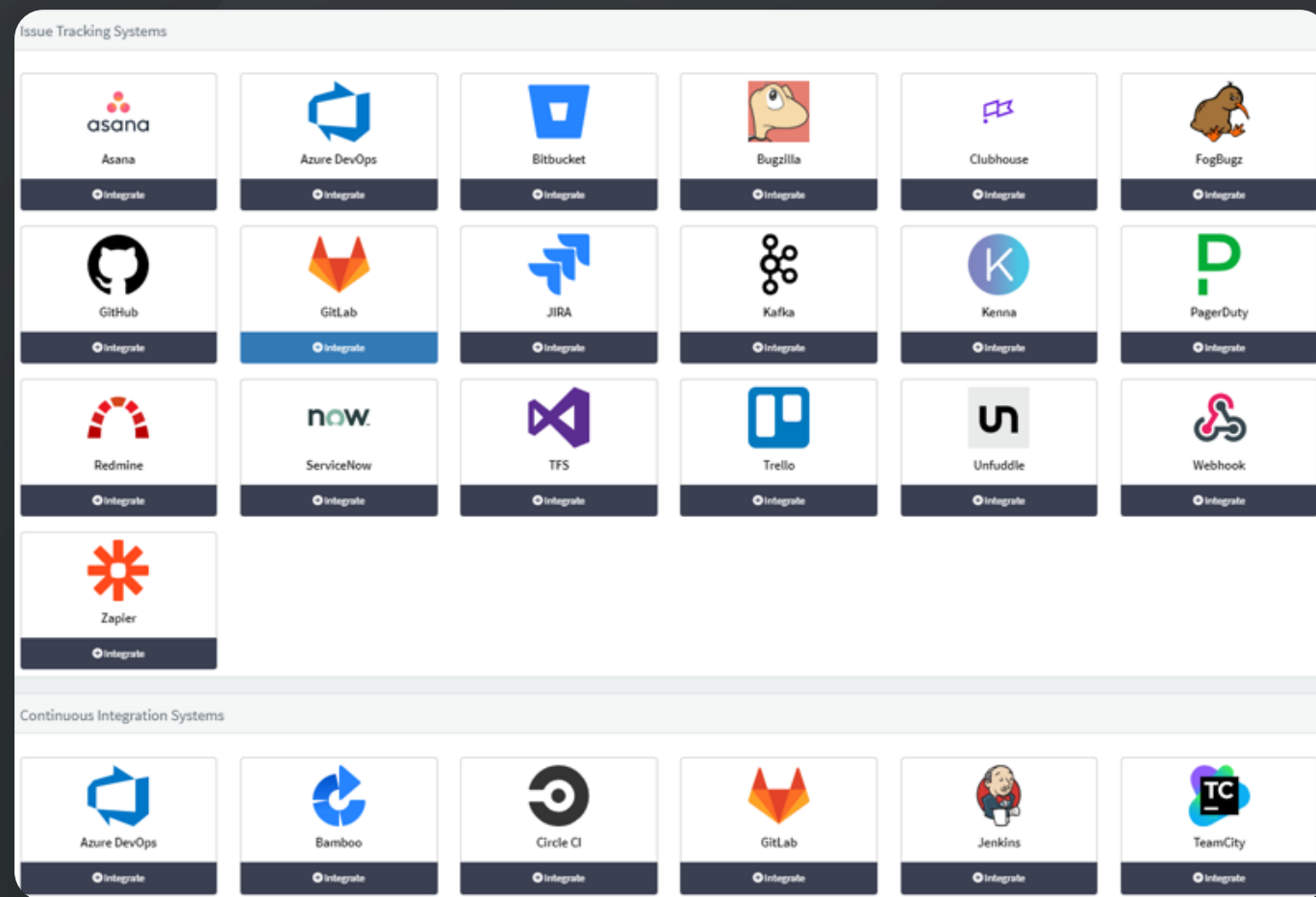
Системы трекинга задач



CI/CD



API



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.

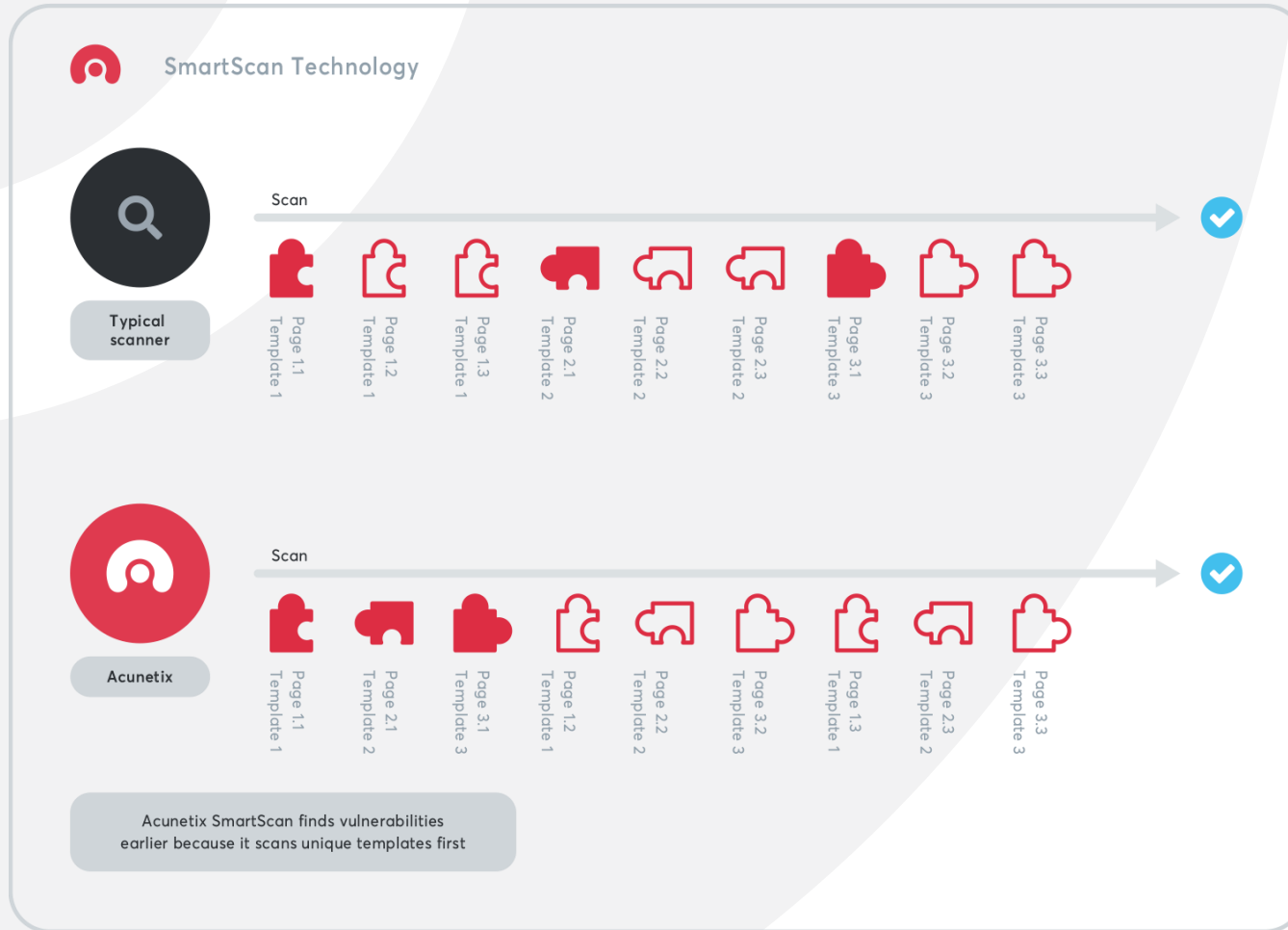


Технология SmartScan

Большинство приложений и веб-сайтов состоит из огромного числа страниц и интерфейсов, основанных на одних и тех же или схожих шаблонах.

Одинаковый шаблон страницы обычно означает наличие одинаковых уязвимостей

Acunetix сначала сканирует уникальные страницы, обнаруживая до 80% уязвимостей за первые 20% скана.



AcuMonitor находит скрытые уязвимости

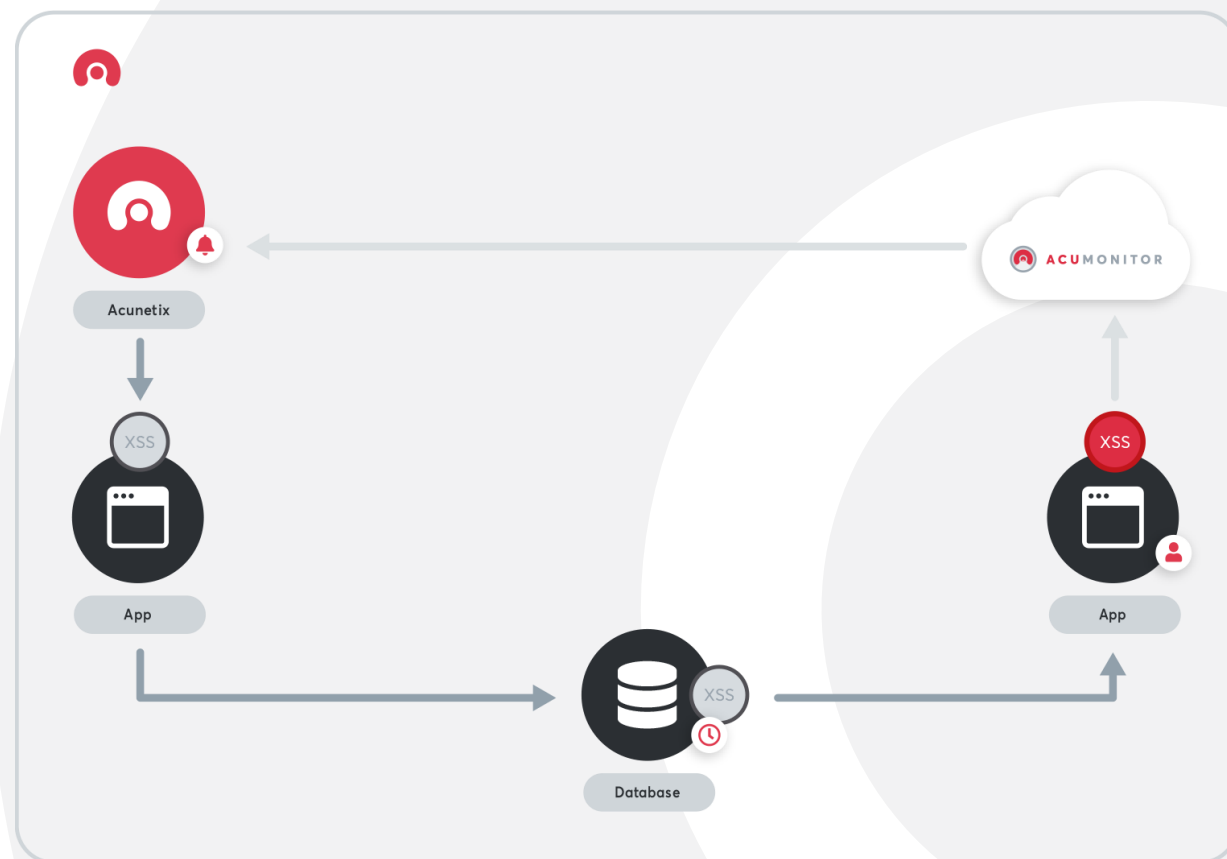
Acunetix может обнаружить скрытые уязвимости, проверяя реакцию веб-приложения на внешние запросы изнутри.

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.



ACUMONITOR





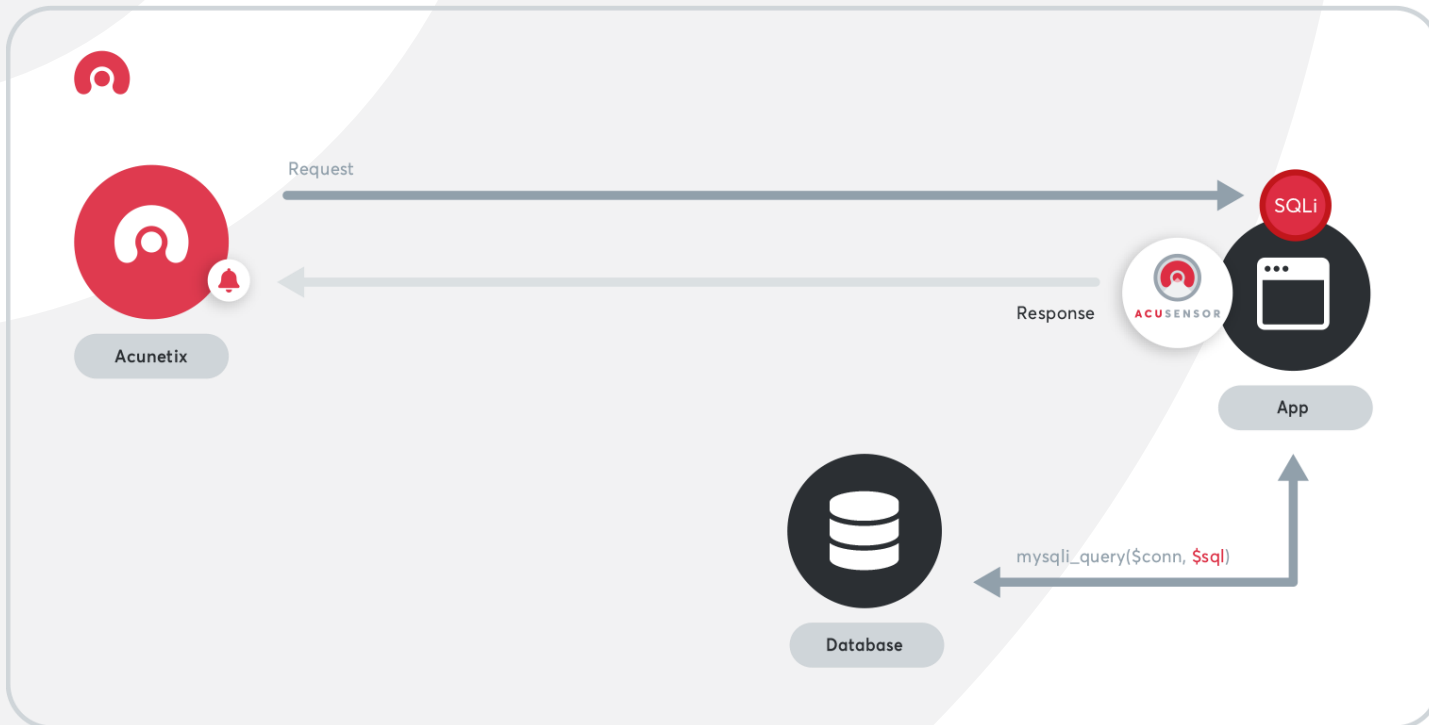
ACUSENSOR

AcuSensor покажет проблему в коде

Acunetix может выполнять роль инструмента для сканирования интерактивных приложений (IAST).

Достаточно установить AcuSensor на сервер – это компонент для PHP, Java и ASP.NET.

AcuSensor проверяет, на какой строке кода проявилась та или иная уязвимость, позволяя быстрее ее найти, устранить и добавить проверку в ваш процесс разработки, чтобы та же проблема не появилась в новом релизе.





ACUSENSOR

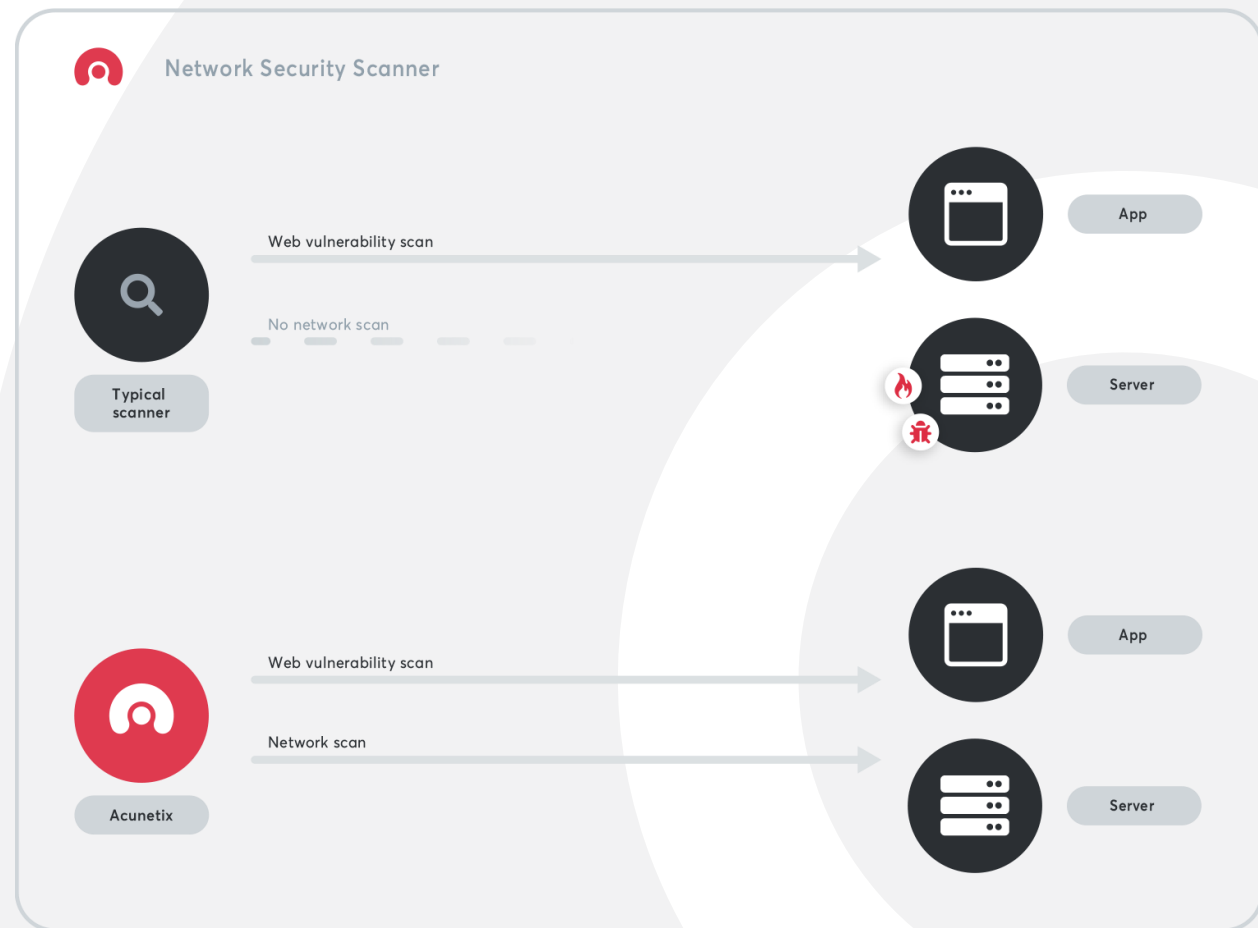
обнаруживает

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

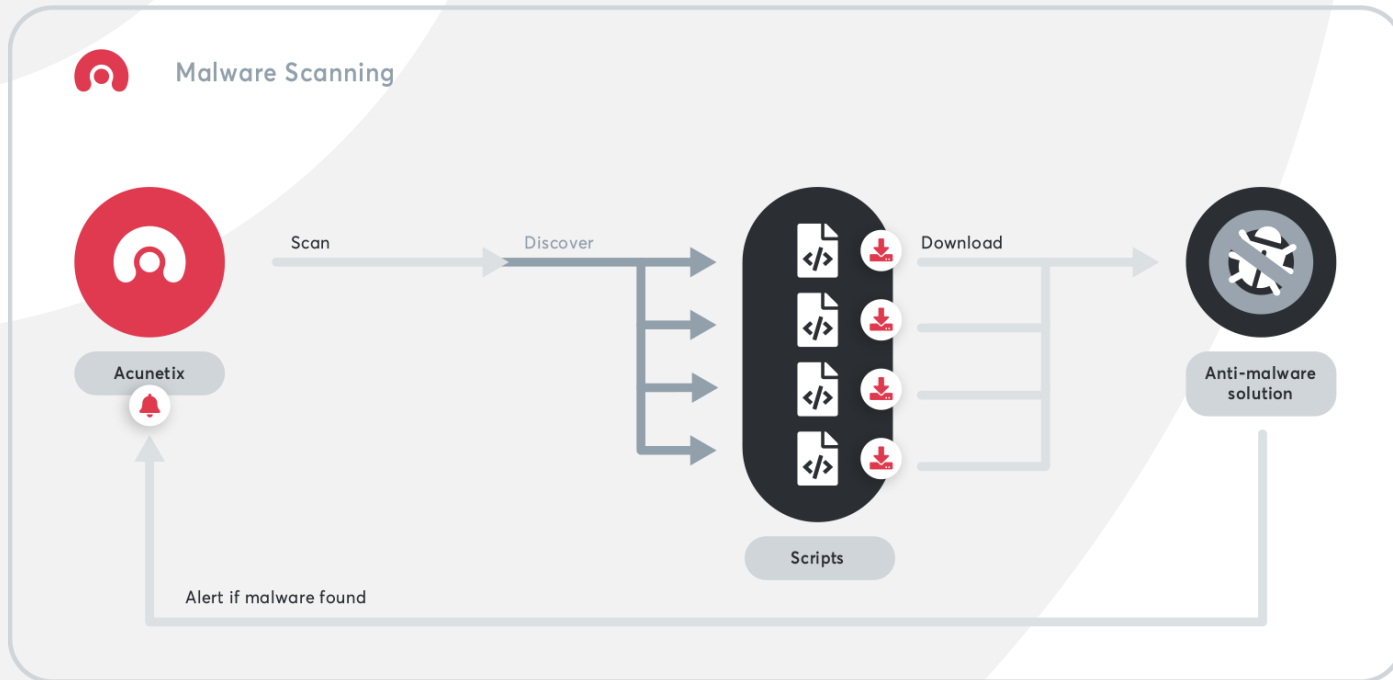
- Изменение файлов
- Загрузку файлов
- Инъекции кода PHP
- Перезапись глобальных переменных
- XSS
- SQL-инъекции
- ...и так далее

Сканирование сети

- Acunetix интегрируется с сканером сетевых уязвимостей OpenVAS
- Обнаруживает более 50,000 различных типов уязвимостей.
- Результаты сканирования сети и веб-приложений попадают в единый интерфейс с удобным распределением задач и интеграцией с CI/CD
- Сканирование сети доступно как для внутренних сканов, так и для скана из облака – проверьте свою сеть со всех сторон
- Бесплатная функция для владельцев лицензии Premium



Обнаружение вредоносного кода



- Acunetix использует базы данных от Google и Yandex, чтобы обнаруживать включения вредоносных ссылок и скриптов в код страницы.
- Дополнительно при установке на Windows используется Windows Defender для сканирования всего загруженного содержимого с веб-сайта.
- На Linux, Acunetix использует для той же цели антивирус ClamAV.

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

Directory traversal

Vulnerability Description ▲

This script is possibly vulnerable to directory traversal attacks.

Directory Traversal is a vulnerability which allows attackers to access restricted directories and read files outside of the web server's root directory.

The vulnerability affects **<http://testphp.vulnweb.com/showimage.php>** , file

Discovered by **Directory traversal**

Attack Details ▲

URL encoded GET input **file** was set to **../../../../../../../../../../../../../../../../proc/version**

File contents found:

```
Linux version 2.6.32-46-server (buildd@lamiak) (gcc version 4.4.3
```

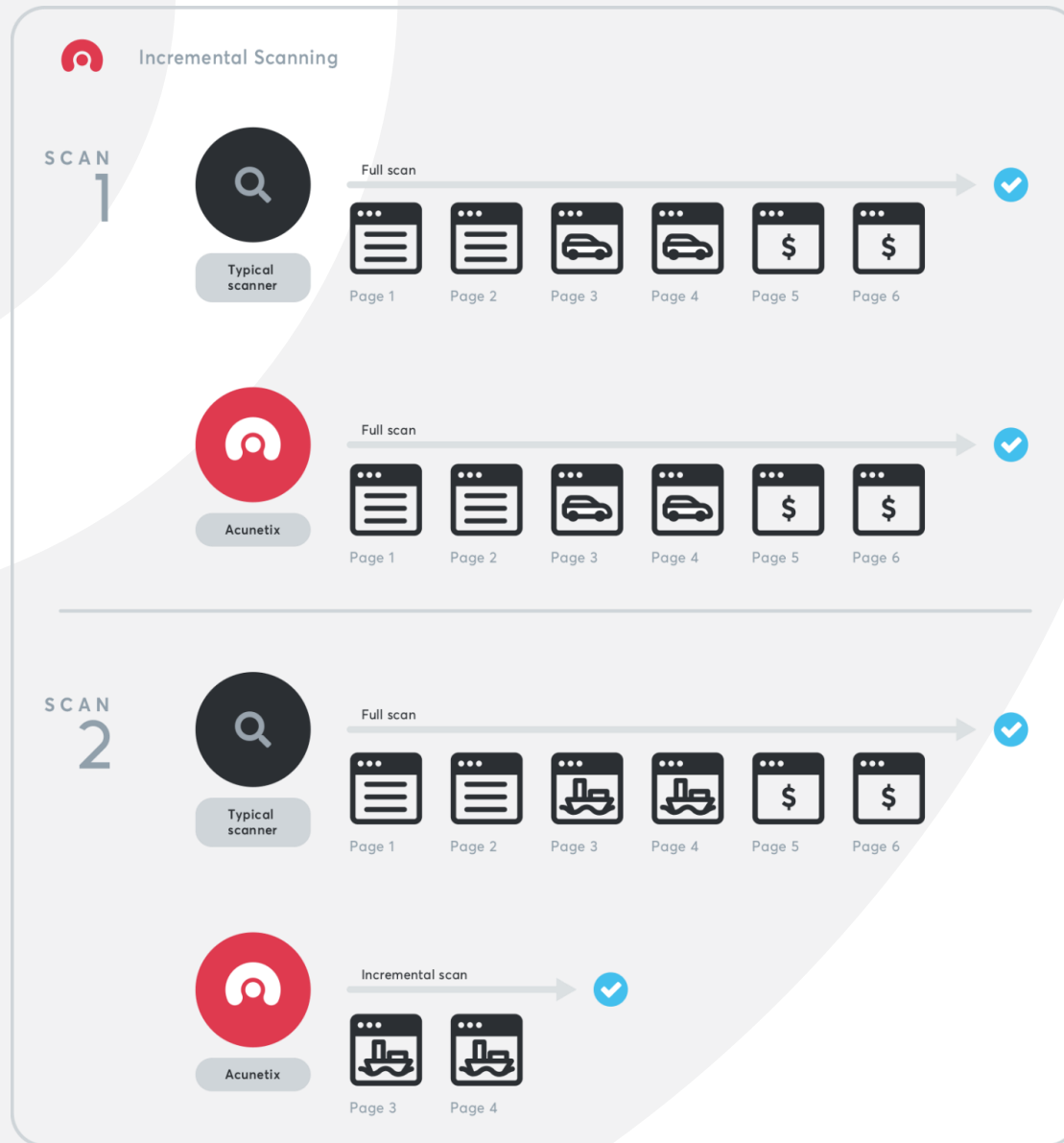
Proof of Exploit

```
File - /proc/version
```

```
Linux version 2.6.32-46-server (buildd@lamiak) (gcc version 4.4.3 (Ubuntu  
4.4.3-4ubuntu5.1) ) #108-Ubuntu SMP Thu Apr 11 16:11:15 UTC 2013
```

Инкрементальное сканирование

- Acunetix одинаково хорошо сканирует как небольшие веб-сайты, так и особо сложные веб-приложения благодаря инкрементальному сканированию.
- При повторном сканировании Acunetix в первую очередь проверит только измененные части веб-приложения
- За счет такой оптимизации экономится до 90% времени сканирования. Особенно полезно при включении Acunetix в ваш процесс CI/CD.



Подходит для компаний любых масштабов

rietsparker
STANDARD

acunetix

acunetix 360

rietsparker
ENTERPRISE

Специалист
ИБ,
консультант

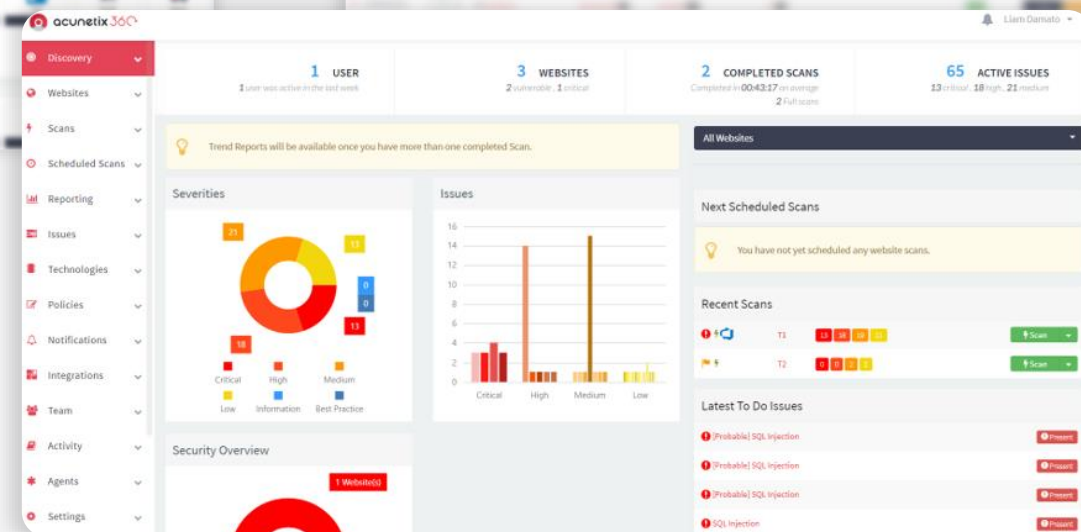
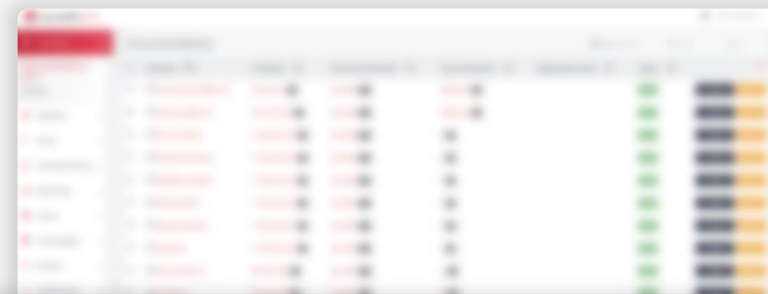
Малый
бизнес

Средний и
крупный бизнес

Особо крупные
организации

Познакомьтесь с продуктом

- Оставьте заявку на демонстрацию продуктов «живьем». Наш специалист покажет интерфейс, объяснит доступные функции и ответит на ваши вопросы.
- Запросите ключ для самостоятельного тестирования – просканируйте ваши веб-приложения, получите первые отчеты и примите решение о включении контроля уязвимостей в ваш процесс разработки
- Расскажите нам о ваших целях, и мы подготовим план пилота и интеграции продукта в вашу сеть



Спасибо!

dm@afi-d.ru
www.Acunetix.com