Валидация структурных типов

Самосадный Кирилл
https://t.me/kirsamosad
samosad@seclab.cs.msu.su

МГУ 2018

Валидация структурных типов

Структурный тип:

- YAML, JSON, XML, …
- PNG, JPG, PDF, DOC, …

Валидация структурных типов

- Метод получения данных веб-приложением / назначение:
  - POST-параметры, является протоколом передачи параметров
  - FileUpload, является загружаемым пользовательским контентом
- FileUpload, что может пойти не так?
  - DoS по места в хранилище
  - Stored XSS
  - RCE
  - Экзотика (см. ZIP-формат)
- Как побороться с Stored XSS архитектурно? А с RCE?

Валидация структурных типов - подходы

- Валидация с использованием парсеров – JSON/XML/HTML
- Валидация сторонней утилитой – картинки/аудио/видео
- Плохо:
  - Писать свои парсеры
  - Использовать небезопасные парсеры, позволяющие выполнять код (PyYaml и Ruby Yaml)
  - Использовать eval
  - Использовать десериализацию

Использование сторонних утилит

- Какие риски от использования популярных утилит?
  - ImageMagic/FFMPEG
  - OpenSSL
  - wget/curl
- Рациональный подход: предполагаем, что во внешнем сложном компоненте есть RCE
- Варианты:
  - используем wrapper (самое простое и небезопасное)
  - используем утилиту в sandbox’е (firejail, AppDomain.CreateDomain, mbox, docker и т.п.)
  - микросервис: используем отдельный узел и оформляем API уровня HTTP
  - не рекомендуется использовать chroot

DEMO: File Upload

Валидация загружаемых файлов

- Проверка имени и расширения файла по белому списку
- Проверка типа файла:
  - заголовок MIME
  - сигнатура типа файла (file magic number)
  - специфичная для типа файла валидация аналогично структурному типу
- Нужно учитывать:
  - ограничения на размер файлов
  - ограничение на имена файлов (длина, разрешённые символы, служебные имена)
  - место хранения файлов (не рекомендуется загружать в webroot)
  - исполнение файла
  - специфику – например, ZIP (символические ссылки, бомбы)
- Что может сделать архитектор, и что – devops/admin

SSRF и задача валидации URL

- Приложение получает URL от пользователя, делает запрос по нему и сохраняет содержимое; что может пойти не так?
- А вот что
  - сканирование портов внутренней сети
  - отправка HTTP-запросов во внутреннюю сеть (а там - микросервисная архитектура)
  - чтение локальных файлов
  - DoS через удержание сетевого соединения или исчерпания места
  - RCE

Литература

- PoC||GTFO 15, статьи про полиглоты
  - https://www.alchemistowl.org/pocorgtfo/pocorgtfo15.pdf
- PNG IDAT Payload Generator
  - https://github.com/huntergregal/PNG-IDAT-Payload-Generator
- ImageTragic
  - https://imagetragick.com/
- Атаки на видеоконвертеры: год спустя (видео доклада)
  - https://www.youtube.com/watch?v=dGnDIzet224