Лаборатория безопасности
Информационных систем
ВМК МГУ имени М. В. Ломоносова

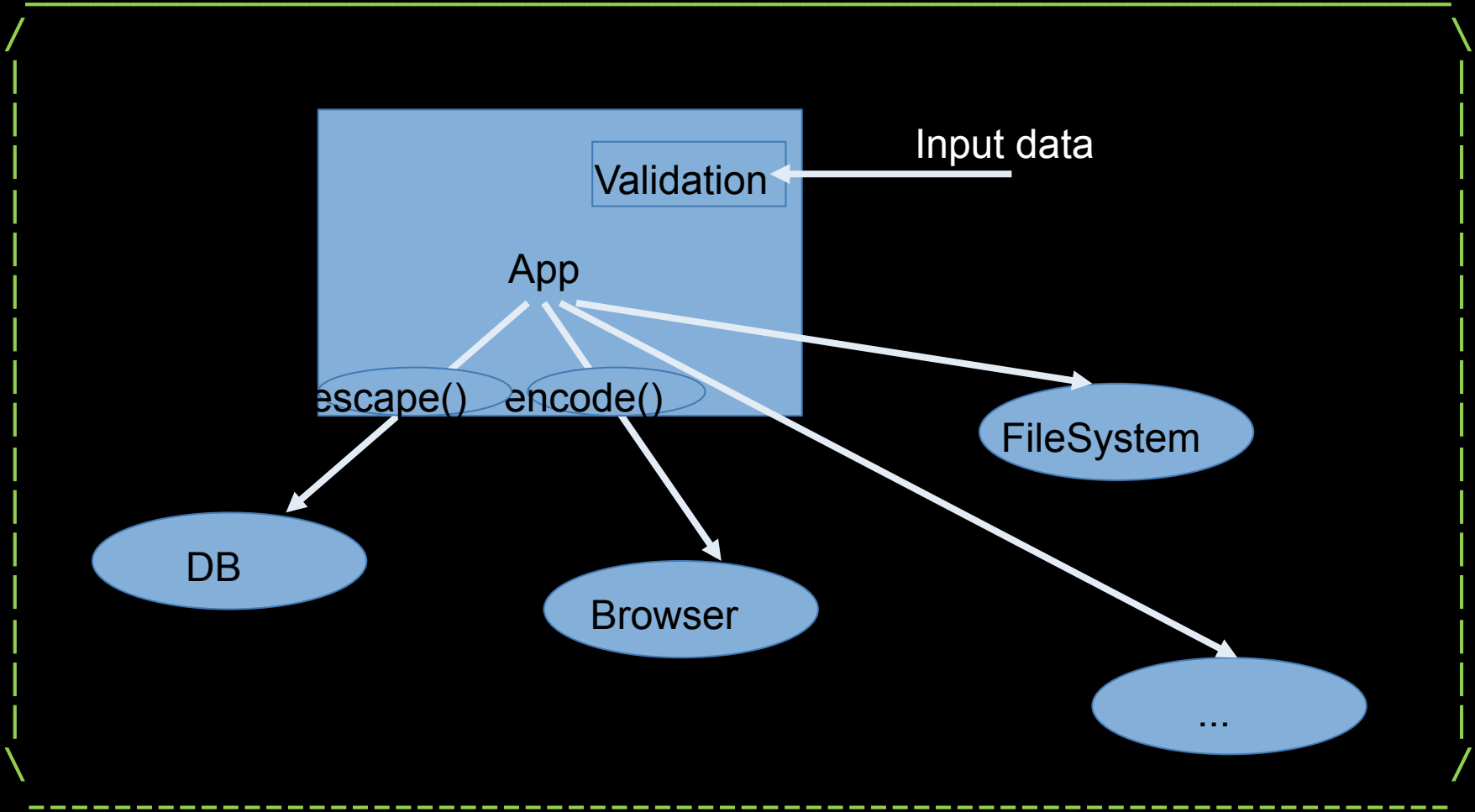
фильтры обработки входных данных как источники уязвимостей

Порхун Анастасия,
аспирантка ВМК МГУ

Обработка входных данных

- Некорректная обработка входных данных
- Порождает injection-класс атак
- Методы борьбы на уровне кода:
  - Валидация
    - Проверка на вхождение в белый список
    - Проверка на вхождение в черный список
    - Приведение к типу
  - Санитизация

Процесс обработки входных данных



File Upload

- Примеры сервисов
  - Загрузка аватарки в социальную сеть
  - Видео на youtube
  - Dropbox-like сервисы
  - Онлайн-сервисы для преобразований файлов

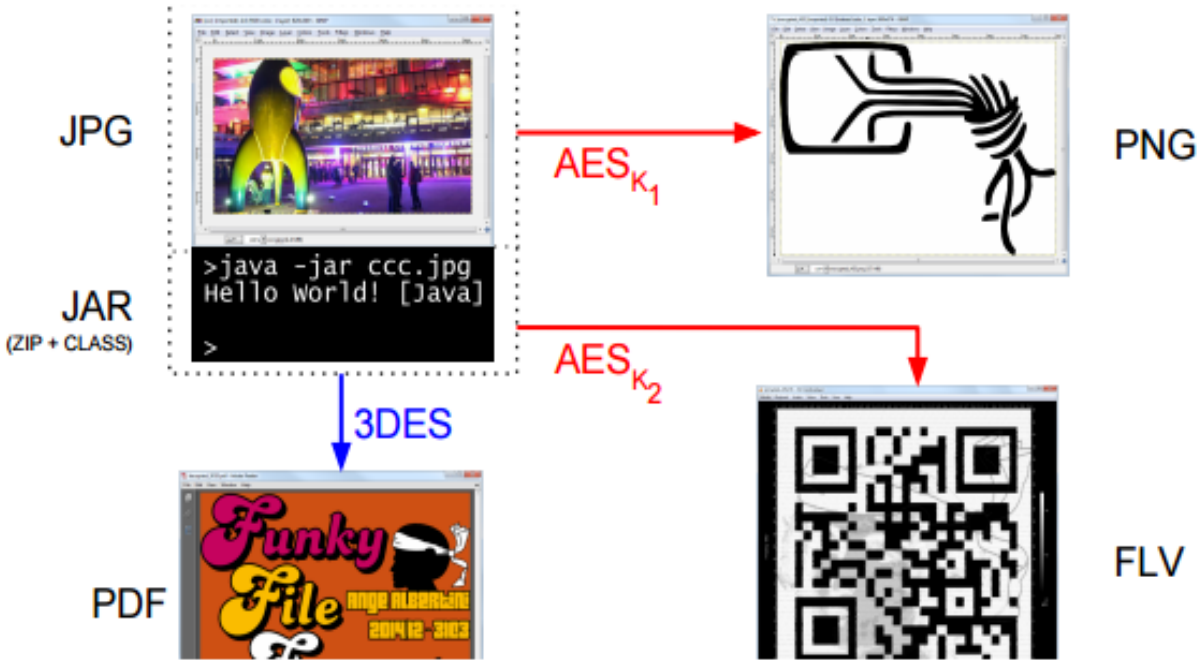
- Преобразования
  - Преобразования типов
  - Шифрование/расшифрование
  - Сжатие

Обработка

Как обрабатывать загружаемые файлы?

- Расширение
- Имя файла
- Тип контента (header, magic number, api)

Примеры обработки



Поиск уязвимостей

- Хочется искать нестандартные валидации в коде приложений статическим анализом
- Еще больше хочется проверять найденные валидации (помним про полиморфные файлы)
- Все то же самое для преобразований данных

Подход

- Библиотека обратных преобразований
- Статический анализ кода
- Анализ прохождения dataflow через фильтры
- Умный фаззинг

Ой, все!

- Порхун Анастасия
  - e-mail:anastasia@seclab.cs.msu.su