

Исследование поверхности атаки, скрывающейся за публичным API

Довгалюк Павел Михайлович
ИСП РАН

WebAPI – поверхность атаки

- Злоумышленник обращается к системе через WebAPI
- Backend через другое API общается с
 - СУБД
 - Очередью заданий
 - ...
- Какие API нужно защищать?

Фаззинг сетевого API

- Мутация должна сохранять структуру пакета
- Некоторые ошибки сосредоточены в обработчиках отдельных полей
- Либо собственный мутатор
- Либо фаззинг низкоуровневых функций

SQL-инъекция или XSS

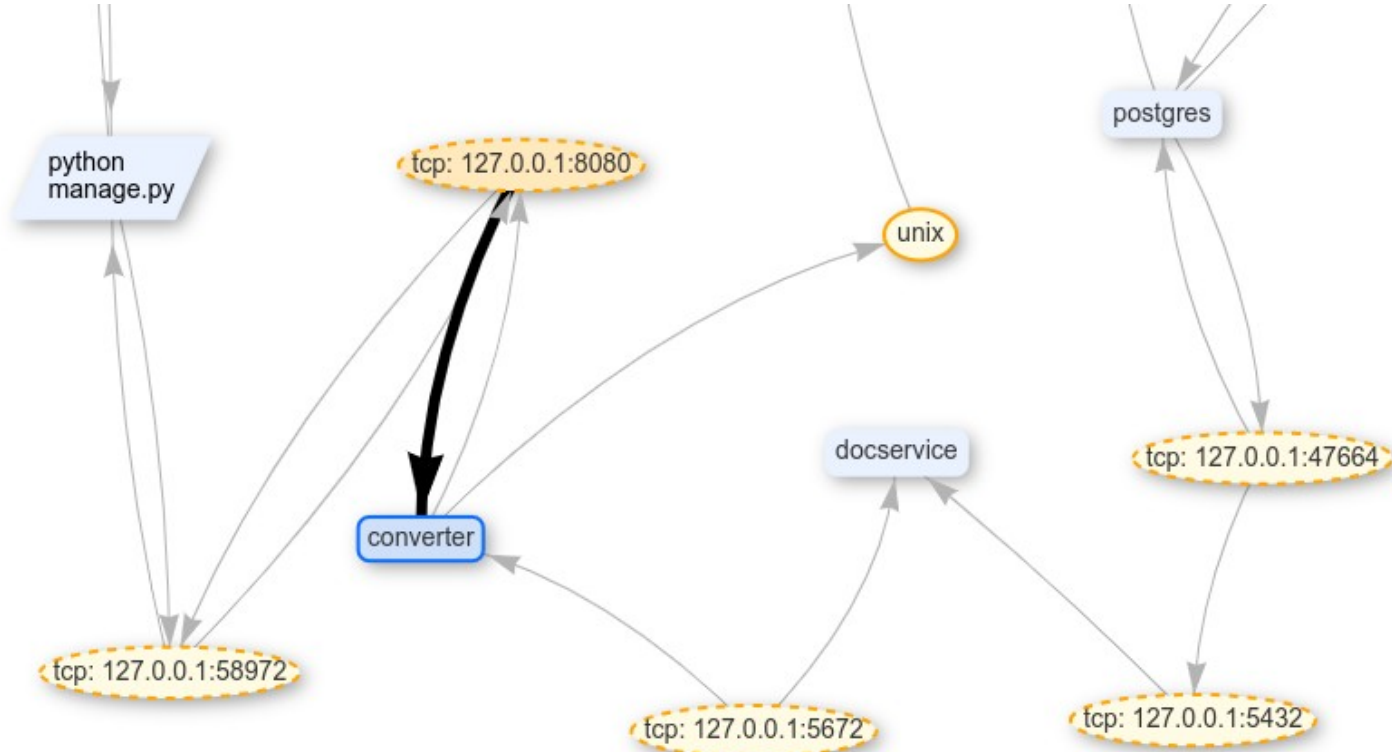
- Сложно нафаззить входящий пакет
 - Несколько вложенных структур
 - Длинная цепочка для проверки срабатывания
- Нужно посмотреть последовательность обработки данных

0000	52 54 00 12 34 56 52 55 0a 00 02 02 08 00 45 00	RT..4VRUE.
0010	00 4c 00 05 00 00 40 11 62 8c 0a 00 02 02 0a 00	.L....@. b.....
0020	02 0f 8b 08 57 f2 00 38 d1 e4 3c 36 3e 4f 63 74	W..8 ..<6>Oct
0030	20 33 30 20 31 30 3a 30 37 3a 31 36 20 6d 79 74	30 10:0 7:16 myt
0040	61 67 3a 20 54 68 69 73 20 69 73 20 61 20 74 65	ag: This is a te
0050	73 74 20 6d 65 73 73 61 67 65	st messa ge

Фаззинг системы с (микро)сервисами

- **Запускать всё в виртуальной машине**
 - Отлеживать (и откатывать) состояние всей VM
 - Следить за падением каждого из сервисов
- **Тестировать сервисы по отдельности**
 - Что именно проверять?
 - Как выбрать API для тестирования?

ONLYOFFICE



- В коде загрузки BMP недостаточно проверок

```
case 24 :  
    if (bf.bfOffBits != 0L) hFile->Seek(off + bf.bfOffBits, SEEK_SET);  
    if (dwCompression == BI_RGB){  
        hFile->Read(info.pImage, head.biSizeImage, 1, GetDIB(), GetDIBLimit()); // read in the pixels  
    } else cx_throw("unknown compression");  
    break;
```

Поверхность атаки

- **Уязвимые места системы**
- **Интерфейсы**
 - Порты
 - Домены
 - Адреса
 - Файлы
- **Программы**
 - Заимствованные компоненты
 - Собственные участки кода

Способы изучения поверхности атаки

- OWASP Noir
- Покрытие кода
- Natch

Spring-petclinic

- **Web-сервис для клиники домашних животных**
 - владельцы
 - питомцы
 - визиты в клинику
- **Простейшее приложение на платформе Spring**
 - ~86 Kb Java-кода
 - есть юнит-тесты

Анализ поверхности атаки petclinic

- Поверхность атаки сложно найти вручную
- В sbom внутри jar-файла описаны 92 зависимости
- Много абстракций
- Глубина стека 200+ функций

Create owner

Owner

First Name

myownerfirst

Last Name

myownerlast

Address

myowneraddr

City

myownercity

Telephone

1234567890

Add Owner

Spring-petclinic

Owner Information

Name	myownerfirst myownerlast
Address	myowneraddr
City	myownercity
Telephone	1234567890

Edit Owner

Add New Pet

Pets and Visits

Поиск поверхности атаки с OWASP Noir

POST /owners/new

body: address=&city=&telephone=

file: ./src/main/java/org/springframework/samples/petclinic/owner/**OwnerController.java (line 75)**

POST /owners/{ownerId}/edit

path: ownerId

body: address=&city=&telephone=

file: ./src/main/java/org/springframework/samples/petclinic/owner/**OwnerController.java (line 138)**

GET /owners/{ownerId}

path: ownerId

file: ./src/main/java/org/springframework/samples/petclinic/owner/**OwnerController.java (line 163)**

Создание записи

```
@PostMapping("/owners/new")
public String processCreationForm(@Valid Owner owner, BindingResult result, RedirectAttributes redirectAttributes) {
    if (result.hasErrors()) {
        redirectAttributes.addFlashAttribute("error", "There was an error in creating the owner.");
        return VIEWS_OWNER_CREATE_OR_UPDATE_FORM;
    }

    this.owners.save(owner);
    redirectAttributes.addFlashAttribute("message", "New Owner Created");
    return "redirect:/owners/" + owner.getId();
}
```

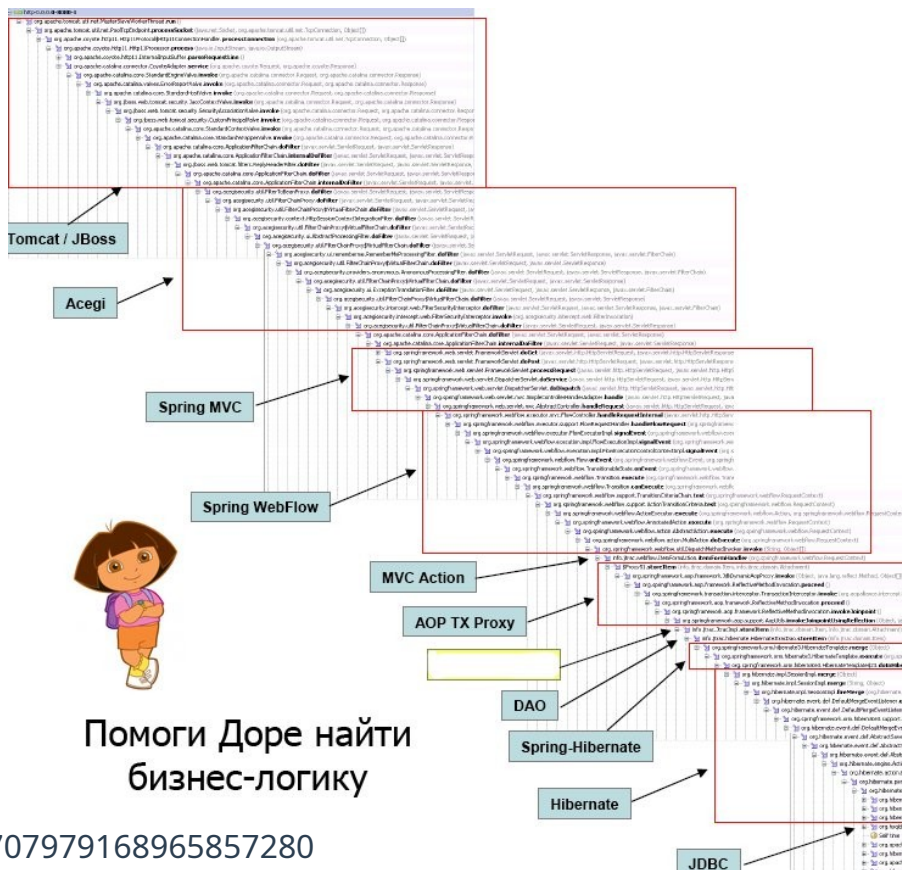
Чтение записи

```
@GetMapping("/owners/{ownerId}")  
public ModelAndView showOwner(@PathVariable("ownerId") int ownerId) {  
    ModelAndView mav = new ModelAndView("owners/ownerDetails");  
    Optional<Owner> optionalOwner = this.owners.findById(ownerId);  
    Owner owner = optionalOwner.orElseThrow(() -> new IllegalArgumentException(  
        "Owner not found with id: " + ownerId + ". Please ensure the ID is correct "));  
    mav.addObject(owner);  
    return mav;  
}
```

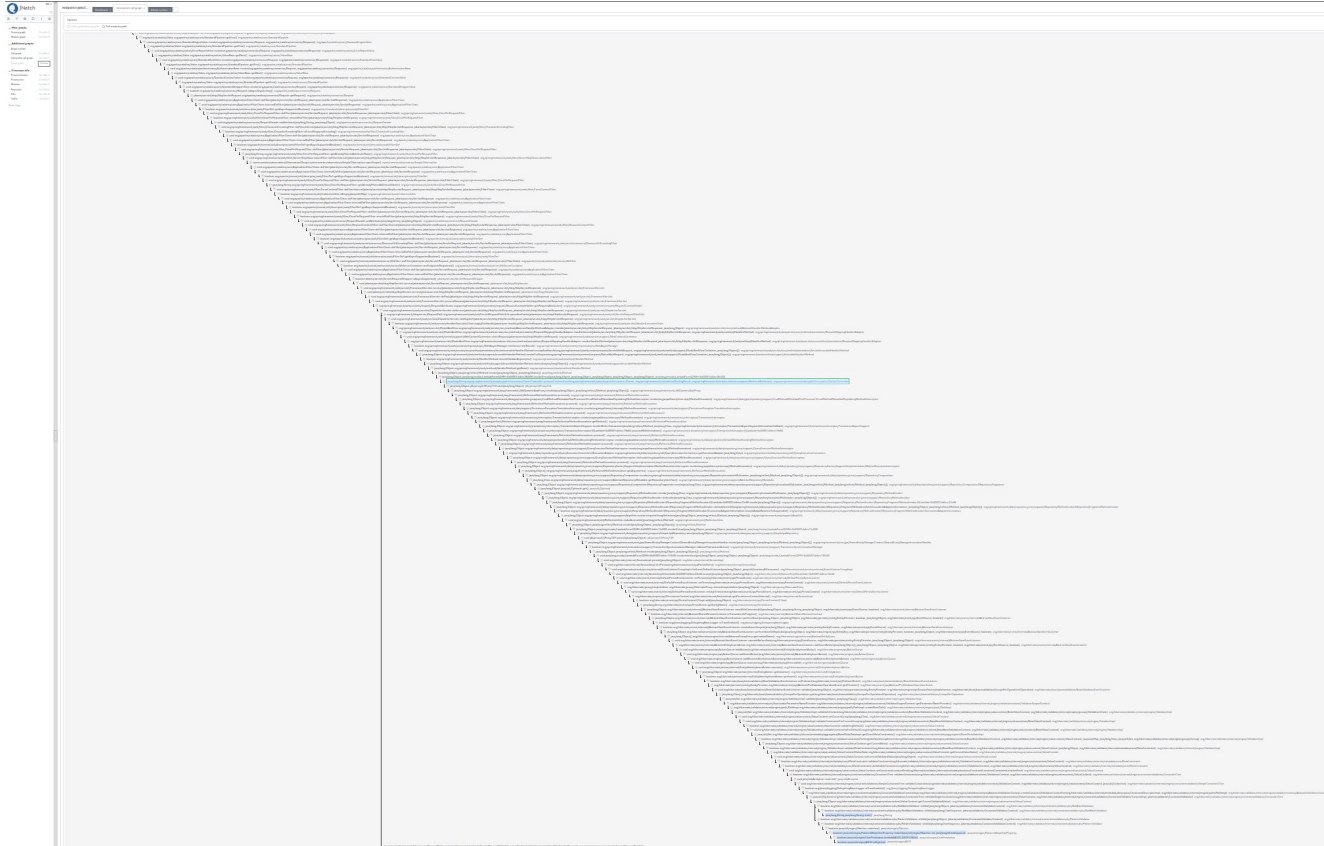

Поккрытие кода

- Неплохое приближение для поверхности атаки
- Но не все найденные функции отвечают за обработку входных данных

На что похож backtrace / call graph



OwnerController



План исследования приложения petclinic

- **В веб-интерфейсе**
 - Создать карточку владельца
 - Просмотреть карточку
- **В инструменте Natch**
 - Пометить полученные данные формы для отслеживания
 - Убедиться, что помеченные данные вернулись назад пользователю при просмотре формы
- **В интерфейсе анализа SMatch**
 - Выбрать интересные модули и функции
- **Фаззинг или поиск багов вручную**

Входные данные

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1:49152/owners/new
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9,ru;q=0.8
Cookie: sidenav-state=pinned; csrftoken=v82VHdvacMs8EraSTY528xP49j9Efbs8; django_language=en-us; session=eyJsb2dnZWRFaW4iOmZhbnHlQ.ZyHHTA.-IH3r05WSU8-MNKDjZzuowFfwcQ; JSESSIONID=D1625244AC34D07B3F8D54F79F77CC51

firstName=myownerfirst&lastName=myownerlast&address=myowneraddr&city=myownercity&telephone=1234567890
```

Страница с карточкой владельца с подсвеченными входными данными

```
<table class="table table-striped">
  <tr>
    <th>Name</th>
    <td><b>myownerfirst myownerlast</b></td>
  </tr>
  <tr>
    <th>Address</th>
    <td>myowneraddr</td>
  </tr>
  <tr>
    <th>City</th>
    <td>myownercity</td>
  </tr>
  <tr>
    <th>Telephone</th>
    <td>1234567890</td>
  </tr>
</table>
```

Изучение поверхности атаки

- Разбор запроса
- Валидация входных данных
- Работа с БД
- Вывод html

Разбор запроса: tomcat

```
⊖ void org/apache/tomcat/util/http/Parameters::processParameters(byte[], int, int) org/apache/tomcat/util/http/Para
└─ ⊖ void org/apache/tomcat/util/http/Parameters::processParameters(byte[], int, int, java/nio/charset/Charset) org
    └─ ⊖ java/lang/String org/apache/tomcat/util/buf/ByteChunk::toString() org/apache/tomcat/util/buf/ByteChunk
        └─ ⊖ java/lang/String org/apache/tomcat/util/buf/ByteChunk::toString(java/nio/charset/CodingErrorAction, jav
            └─ ⊖ boolean org/apache/tomcat/util/buf/AbstractChunk::isNull() org/apache/tomcat/util/buf/AbstractChu
                └─ ⊖ java/lang/String org/apache/tomcat/util/buf/StringCache::toString(org/apache/tomcat/util/buf/Byt
                    └─ ⊖ java/lang/String org/apache/tomcat/util/buf/ByteChunk::toStringInternal(java/nio/charset/Codi
                        └─ ⊖ java/nio/CharBuffer java/nio/charset/Charset::decode(java/nio/ByteBuffer) java/nio/charset
                            └─ ⊖ java/nio/charset/CharsetDecoder sun/nio/cs/ThreadLocalCoders::decoderFor(java/lang/C
                                └─ ⊖ java/nio/CharBuffer java/nio/charset/CharsetDecoder::decode(java/nio/ByteBuffer) j
                                    └─ java/nio/charset/CoderResult java/nio/charset/CharsetDecoder::decode(java/nio/Byt
```


Валидация входных данных: hibernate

```
- ⊖ org/hibernate/validator/internal/engine/constraintvalidation/ConstraintValidatorContextImpl org/hibernate/validator/internal/engine/valida
  L ⊖ java/util/Optional org/hibernate/validator/internal/engine/constraintvalidation/ConstraintTree::validateSingleConstraint(org/hibernate/va
    L ⊖ java/lang/Object org/hibernate/validator/internal/engine/valuecontext/ValueContext::getCurrentValidatedValue() org/hibernate/valid
      L ⊖ boolean org/hibernate/validator/internal/constraintvalidators/bv/NotBlankValidator::isValid(java/lang/Object, jakarta/validation/Con
        L ⊖ boolean org/hibernate/validator/internal/constraintvalidators/bv/NotBlankValidator::isValid(java/lang/CharSequence, jakarta/va
          L java/lang/String java/lang/String::trim() java/lang/String
        L ⊖ boolean org/hibernate/validator/internal/constraintvalidators/bv/PatternValidator::isValid(java/lang/Object, jakarta/validation/Con
          L ⊖ boolean org/hibernate/validator/internal/constraintvalidators/bv/PatternValidator::isValid(java/lang/CharSequence, jakarta/vali
            L ⊖ boolean java/util/regex/Matcher::matches() java/util/regex/Matcher
              L ⊖ boolean java/util/regex/Pattern$BmpCharProperty::match(java/util/regex/Matcher, int, java/lang/CharSequence) java/u
                L ⊖ boolean java/util/regex/CharPredicates::lambda$ASCII_DIGIT$18(int) java/util/regex/CharPredicates
                  L boolean java/util/regex/ASCII::isDigit(int) java/util/regex/ASCII
```

Вставка значений в БД: h2

```
⊖ void org/h2/mvstore/db/MVTable::addRow(org/h2/engine/SessionLocal, org/h2/result/Row) org/h2/mvstore/db/MVTable
  L ⊖ java/lang/Object java/util/ArrayList$Itr::next() java/util/ArrayList$Itr
    L ⊖ void org/h2/mvstore/db/MVSecondaryIndex::add(org/h2/engine/SessionLocal, org/h2/result/Row) org/h2/mvstore/db/MVSecondaryIndex
      L ⊖ boolean org/h2/index/Index::needsUniqueCheck(org/h2/result/SearchRow) org/h2/index/Index
        L ⊖ java/lang/Object org/h2/mvstore/tx/TransactionMap::put(java/lang/Object, java/lang/Object) org/h2/mvstore/tx/TransactionMap
          L ⊖ java/lang/Object org/h2/mvstore/tx/TransactionMap::set(java/lang/Object, java/lang/Object) org/h2/mvstore/tx/TransactionMap
            L ⊖ void org/h2/mvstore/tx/TxDecisionMaker::initialize(java/lang/Object, java/lang/Object) org/h2/mvstore/tx/TxDecisionMaker
              L ⊖ java/lang/Object org/h2/mvstore/tx/TransactionMap::set(java/lang/Object, org/h2/mvstore/tx/TxDecisionMaker, int) org/h2/mvstore/tx/TransactionMap
                L ⊖ java/lang/Object org/h2/mvstore/MVMap::operate(java/lang/Object, java/lang/Object, org/h2/mvstore/MVMap$DecisionMaker) org/h2/mvstore/MVMap
                  L ⊖ boolean org/h2/mvstore/RootReference::isLocked() org/h2/mvstore/RootReference
                    L ⊖ org/h2/mvstore/CursorPos org/h2/mvstore/CursorPos::traverseDown(org/h2/mvstore/Page, java/lang/Object) org/h2/mvstore/CursorPos
                      L ⊖ int org/h2/mvstore/db/RowDataType::binarySearch(org/h2/result/SearchRow, java/lang/Object, int, int) org/h2/mvstore/db/RowDataType
                        L ⊖ int org/h2/mvstore/db/RowDataType::binarySearch(org/h2/result/SearchRow, org/h2/result/SearchRow[], int, int) org/h2/mvstore/db/RowDataType
                          L ⊖ int org/h2/mvstore/db/RowDataType::compareSearchRows(org/h2/result/SearchRow, org/h2/result/SearchRow) org/h2/mvstore/db/RowDataType
                            L ⊖ int org/h2/mvstore/db/ValueDataType::compareValues(org/h2/value/Value, org/h2/value/Value, int) org/h2/mvstore/db/ValueDataType
```

Рендер страницы: thymeleaf

```
⊖ void org/thymeleaf/spring6/view/ThymeleafView::render(java/util/Map, jakarta/servlet/http/HttpServletRequest, jakarta/servlet/http/HttpServletResponse)
  L ⊖ void org/thymeleaf/spring6/view/ThymeleafView::renderFragment(java/util/Set, java/util/Map, jakarta/servlet/http/HttpServletRequest, jakarta/servlet/http/HttpServletResponse)
    L ⊖ java/io/PrintWriter jakarta/servlet/ServletResponseWrapper::getWriter() jakarta/servlet/ServletResponseWrapper
      L ⊖ void org/thymeleaf/TemplateEngine::process(java/lang/String, java/util/Set, org/thymeleaf/context/IContext, java/io/Writer) org/thymeleaf/TemplateEngine
        L ⊖ void org/thymeleaf/TemplateEngine::process(org/thymeleaf/TemplateSpec, org/thymeleaf/context/IContext, java/io/Writer) org/thymeleaf/TemplateEngine
          L ⊖ void org/apache/catalina/connector/CoyoteWriter::flush() org/apache/catalina/connector/CoyoteWriter
            L ⊖ void org/apache/catalina/connector/OutputBuffer::flush() org/apache/catalina/connector/OutputBuffer
              L ⊖ void org/apache/catalina/connector/OutputBuffer::doFlush(boolean) org/apache/catalina/connector/OutputBuffer
                L ⊖ void org/apache/catalina/connector/OutputBuffer::flushCharBuffer() org/apache/catalina/connector/OutputBuffer
                  L ⊖ void org/apache/catalina/connector/OutputBuffer::realWriteChars(java/nio/CharBuffer) org/apache/catalina/connector/OutputBuffer
                    L ⊖ void org/apache/tomcat/util/buf/C2BConverter::convert(java/nio/CharBuffer, java/nio/ByteBuffer) org/apache/tomcat/util/buf/C2BConverter
                      L ⊖ java/nio/charset/CoderResult java/nio/charset/CharsetEncoder::encode(java/nio/CharBuffer, java/nio/ByteBuffer) org/apache/tomcat/util/buf/C2BConverter
                        L ⊖ java/nio/charset/CoderResult sun/nio/cs/UTF_8$Encoder::encodeLoop(java/nio/CharBuffer, java/nio/ByteBuffer) org/apache/tomcat/util/buf/C2BConverter
                          L ⊖ java/nio/charset/CoderResult sun/nio/cs/UTF_8$Encoder::encodeArrayLoop(java/nio/CharBuffer, java/nio/ByteBuffer) org/apache/tomcat/util/buf/C2BConverter
                            L ⊖ int java/lang/System$2::encodeASCII(char[], int, byte[], int, int) java/lang/System$2
                              L int java/lang/StringCoding::implEncodeAsciiArray(char[], int, byte[], int, int) java/lang/StringCoding
```

Экранирование вывода: unescape

```
⊖ java/lang/String org/thymeleaf/util/EscapedAttributeUtils::unescapeAttribute(org/thymeleaf/templatemode/Templa
  L ⊖ void org/thymeleaf/standard/processor/AbstractStandardExpressionAttributeTagProcessor::doProcess(org/thyme
    L ⊖ java/lang/Object org/thymeleaf/standard/expression/Expression::execute(org/thymeleaf/context/IExpression
      ⊕ org/thymeleaf/standard/expression/IStandardVariableExpressionEvaluator org/thymeleaf/standard/expres
      L ⊖ void org/thymeleaf/standard/processor/StandardTextTagProcessor::doProcess(org/thymeleaf/context/ITer
        L ⊖ java/lang/String org/thymeleaf/standard/processor/StandardTextTagProcessor::produceEscapedOutput
          L ⊖ java/lang/String org/unescape/html/HtmlEscape::escapeHtml4Xml(java/lang/String) org/unescap
            L ⊖ java/lang/String org/unescape/html/HtmlEscape::escapeHtml(java/lang/String, org/unescape/
              L ⊖ java/lang/String org/unescape/html/HtmlEscapeUtil::escape(java/lang/String, org/unescap
                L char java/lang/String::charAt(int) java/lang/String
```

unescape

- **HtmlEscapeUtil**
- **Функция escape выглядит не очень сложной**
- **А вот в unescape много ветвлений и циклов**
- **Code smells**
 - escape и unescape существуют в трёх (!) почти одинаковых экземплярах (одна для строк, другая для потоков, третья для массивов)

diff для версий unescape()

1:268,269c

3:252,253c

```
if ((f - (i + 1)) <= 0) {
```

```
    // We weren't able to consume any alphanumeric
```

2:295,297c

```
if (escapei == 0) {
```

```
    // We weren't able to consume any decimal chars
```

```
    writer.write(c1);
```

Фаззинг escape + unescape

```
String result = HtmlEscapeUtil.escape(text,  
    HtmlEscapeType.HTML5_NAMED_REFERENCES_DEFAULT_TO_DECIMAL,  
    HtmlEscapeLevel.LEVEL_2_ALL_NON_ASCII_PLUS_MARKUP_SIGNIFICANT);  
String result2 = HtmlEscapeUtil.unescape(result);  
if (!text.equals(result2)) {  
    System.out.println(" in: " + text);  
    System.out.println("esc: " + result);  
    System.out.println("out: " + result2);  
    throw new Exception();  
}
```


Фаззинг escape + unescape: не-ASCII символы

```
== libFuzzer crashing input ==
MS: 4 ChangeByte-Custom-ChangeByte-Custom-; base unit: e0fbd8cc7b1840b748dfcb6d5628d81739be64de
0x58,0x5c,0x5c,0x5c,0x5c,0xad,0x5c,0xdf,0x81,0x81,0x86,0x3b,0x81,0x5b,0x42,0x81,0x86,0x7e,0x81,0
X\\\\\\\\\\255\\\\337\\201\\201\\206;\\201[B\\201\\206~\\201\\201\\307\\201\\201\\201\\\\221%\\006\\D\\243\\006\\
artifact_prefix='./'; Test unit written to ./crash-c336249dfbd6f7770416e44b6a9d89265f16e4d3
Base64: WfxcXFytXN+BgYY7gVtCgYZ+gYHHgYGBXJElBlxEowZc
in: X\\\\\\\\\\1Æ;UBÆ~Á||Á\\€ \\DÆ\\
esc: X\\\\\\\\\\&#860;&#1985;&AElig;8Ucirc;B&AElig~&Aacute;&#449;&Aacute;\\&#1125; \\D&AElig\\
out: X\\\\\\\\\\1ÆÛBÆ~Á||Á\\€ \\DÆ\\
reproducer_path='./'; Java reproducer written to ./Crash_c336249dfbd6f7770416e44b6a9d89265f16e4d3
```

AElig;	U+000C6	Æ
AElig	U+000C6	Æ
aelig;	U+000E6	æ
aelig	U+000E6	æ

Тест для escape + unescape

```
String text = "\306;\304;\305;";
```

```
System.out.println(text);
```

```
String result = HtmlEscapeUtil.escape(text,  
HtmlEscapeType.HTML5_NAMED_REFERENCES_DEFAULT_TO_DECIMAL,  
HtmlEscapeLevel.LEVEL_2_ALL_NON_ASCII_PLUS_MARKUP_SIGNIFICANT);
```

```
String result2 = HtmlEscapeUtil.unescape(result);
```

```
System.out.println(result);
```

```
System.out.println(result2);
```

Æ;Ä;Å;

ÆÄ;Å;

ÆÄ;Å;

Недетерминированное поведение `escape` + `unescape`

- Преобразование разных символов работает по-разному
- Оказывается, уже есть `issue` и `pull request` от 2023 года на эту тему
- Коммитов, меняющих код, не было с 2018 года

Выводы

- Уязвимые API есть не только снаружи, но и внутри
- Внутренние функции также могут быть доступны злоумышленнику
- Проблемные зависимости быстрее находятся, если знать поверхность атаки

Telegram-канал Natch

- https://t.me/ispras_natch
- Ссылки на документацию и релизы
- Вопросы от пользователей
- Разборы кейсов
- Анонсы вебинаров
- Уведомления о новых релизах
- Собственный стикерпак с нарвалами :)

