

АНТИФИШИНГ

Безопасная разработка и Shift-Left Security:
как далеко влево вы готовы зайти?



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

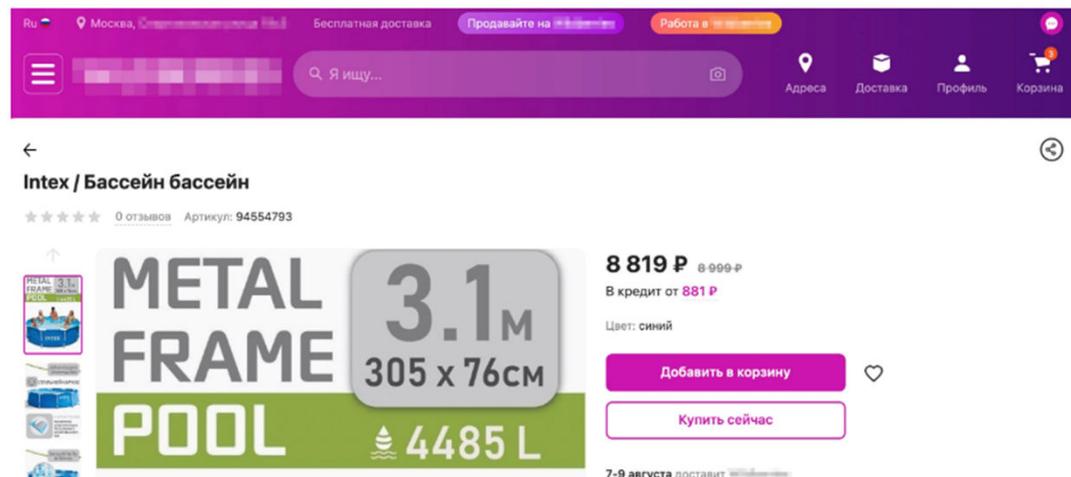
blog.antiphish.ru

Киберкампании

Обнаружена мошенническая кампания, для проведения которой используется популярный маркетплейс.

Схема действий мошенников

1. Мошенники выкладывают на официальный сайт известного маркетплейса несколько товаров. Это может быть все, что угодно: от дачного бассейна до смартфона. Преступники представляются разными продавцами, но используют один и тот же номер.



t.me/antph



Андрей Жаркевич
редактор



Артеми́й Богданов
технический директор



Сергей Волдохин
выпускающий редактор



Askona **Блог**

Клиент в фокусе: как «Аскона» и менила потребительский опыт

..... <

Новости 12.10.20

19:25
СпасеХ отправит первого в историю космического туриста в полет вокруг Луны



Миллиардеры

Читайте о людях, владевших и владеющих крупнейшими состояниями в России и мире

Информационная безопасность
26.01.2022, 00:47

Вирус взял подработкой

В доработанных модулях 1С нашли вредоносный код

👁 33К

💬 4

📖 2 мин.

★

🌐

VK

▶

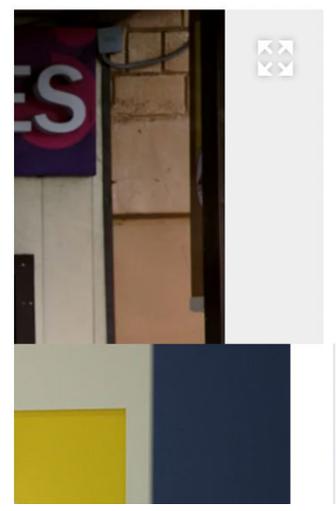
⋮

Данные нескольких десятков компаний были украдены через вредоносный код в модулях 1С, обнаружили в RTM Group. По ее данным, он встраивался в программное обеспечение (ПО) во время доработки модулей у программистов на аутсорсинге. В самой 1С утверждают, что не сталкивались с такими случаями, но, чтобы избежать злоупотреблений, предлагают клиентам обращаться к официальным сертифицированным партнерам. Подобные вещи не всегда происходят умышленно, уточняют эксперты, заражен может быть компьютер самого исполнителя.



Нное

головное дело и регистрировались, а затем уже под изитам. Тем не менее ошеннические схемы ыстром росте, откуда





Стакан TEUR



Bid, €	0,0004 (0,387%)		Ask, €
0,1033	2202700	101094	0,1037
0,1032	88257	164225	0,1038
0,1031	15348	2250530	0,1039
0,1030	67003	105492	0,1040
0,1029	23235	2031	0,1041
0,1028	50740	6210	0,1042
0,1027	55980	6299	0,1043
0,1026	8913	5757	0,1044



Список изменений



Обратная связь



Справка



Чат поддержки



ENG

12:22

21.05.2021



Путаница зависимостей. Как я взломал Apple, Microsoft и десятки других компаний

Код предназначался для внутреннего использования в PayPal, и в его файле package.json, по видимому, содержалась смесь публичных и частных зависимостей — публичные пакеты от npm, а также имена непубличных пакетов, скорее всего, размещённых внутри PayPal. В то время этих имён не было в публичном реестре npm.

<https://habr.com/ru/company/skillfactory/blog/550380/>

```
"dependencies": {  
  "express": "^4.  
  "dustjs-helpers  
  "continuation-l  
  "pplogger": "^0  
  "auth-paypal":  
  "wurfl-paypal":  
  "analytics-payp  
}
```

При загрузке зависимостей менеджеры пакетов npm, pip и gem в основном берут пакеты из основных общедоступных репозиторий NPM, PyPI и RubyGems, которые являются приоритетными.

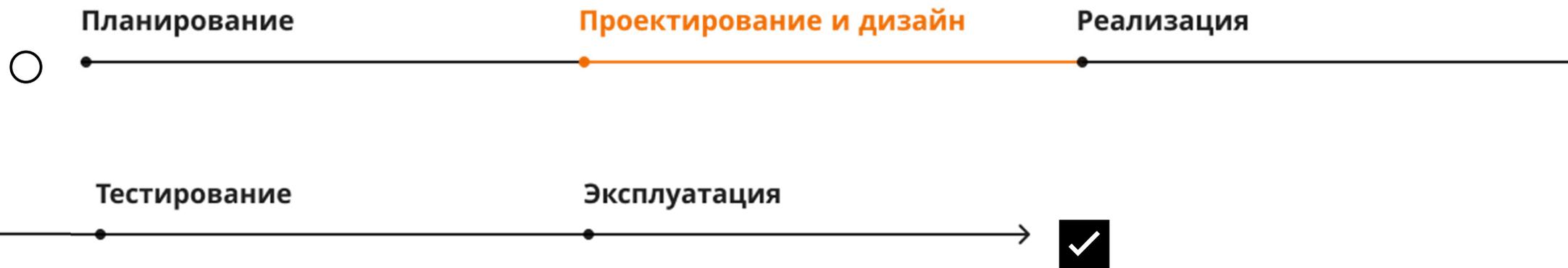
Присутствие похожих пакетов с такими же именами в репозиториях игнорировалось без отображения предупреждений и сообщений администраторов. В PyPI на приоритет загрузки влиял номер версии (была загружена самая последняя версия пакета). В NPM и RubyGems приоритет был только от репозитория.



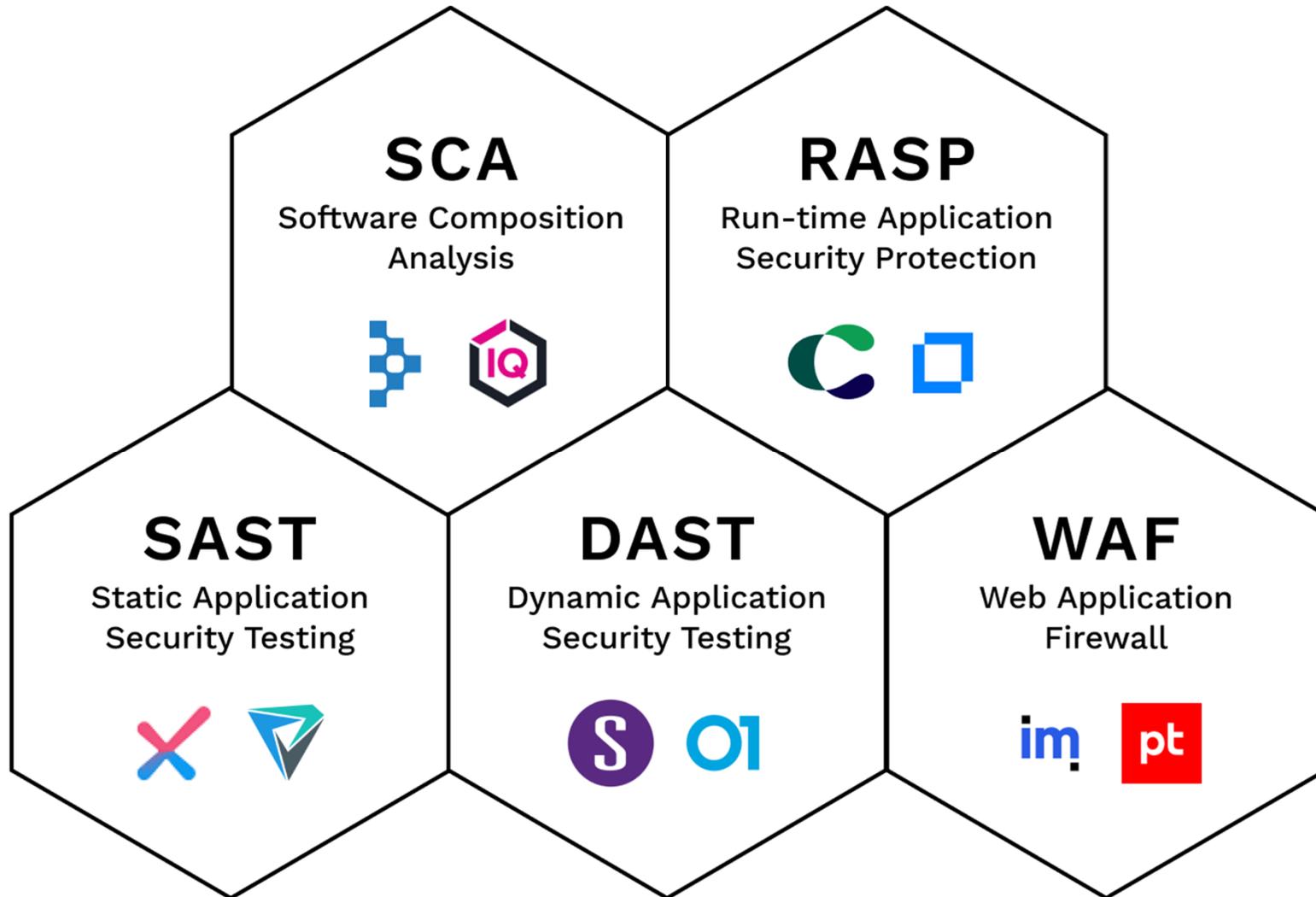
A Что такое Shift-Left Security?

Shift-Left Security – внедрение проверок и практик безопасности в процессе SDLC **так рано и так часто, как это возможно.**

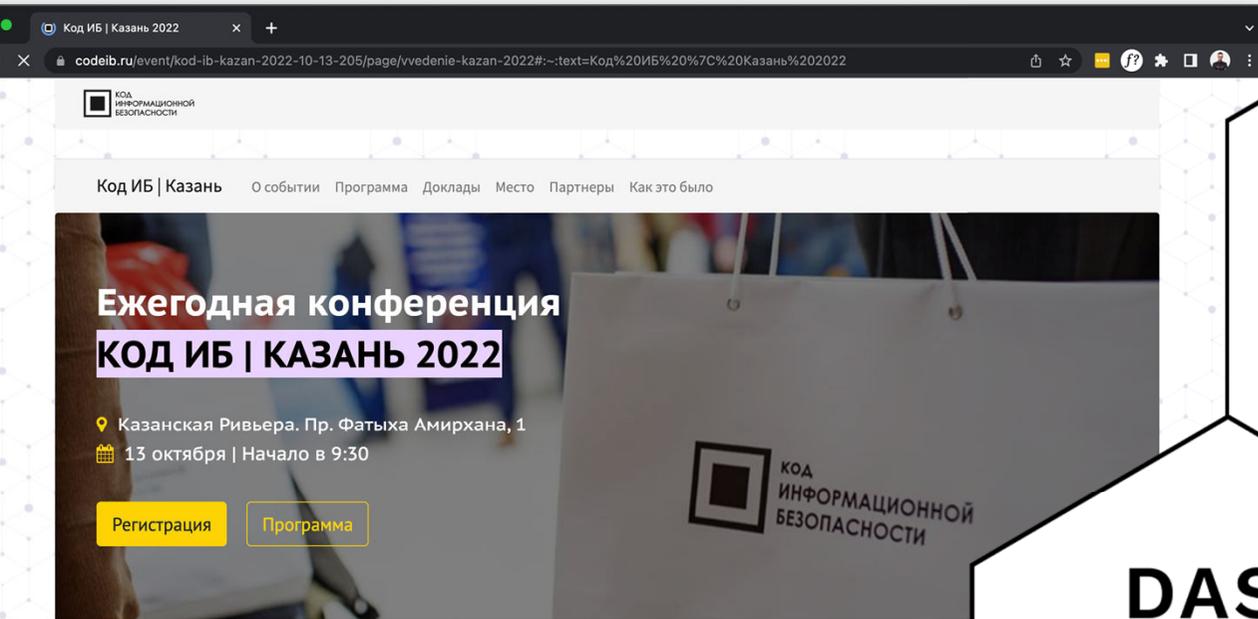
Устранение уязвимостей, **выявленных как можно раньше в процессе разработки,** значительно проще и обходится значительно дешевле



A Какие инструменты делают продукт безопасным?

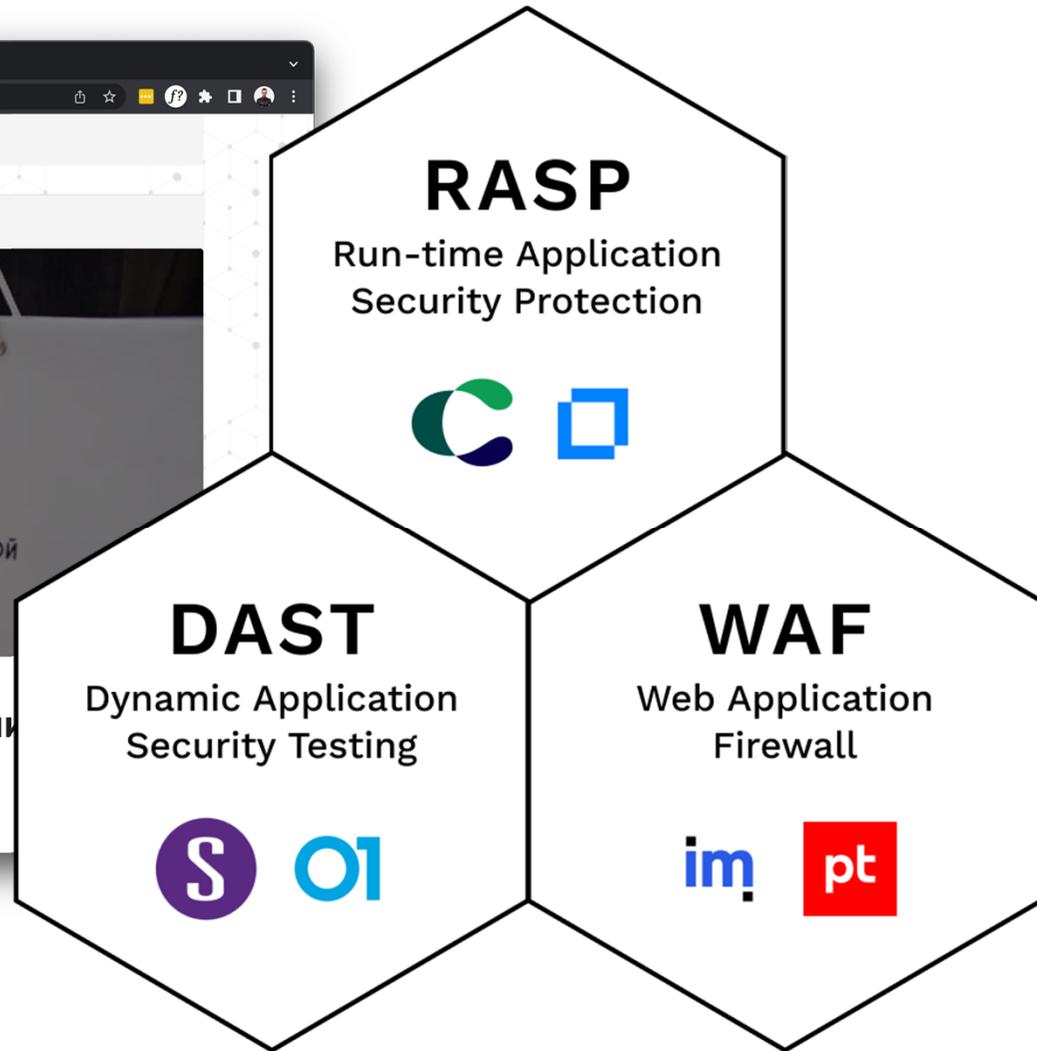


A Какие инструменты делают продукт безопасным?

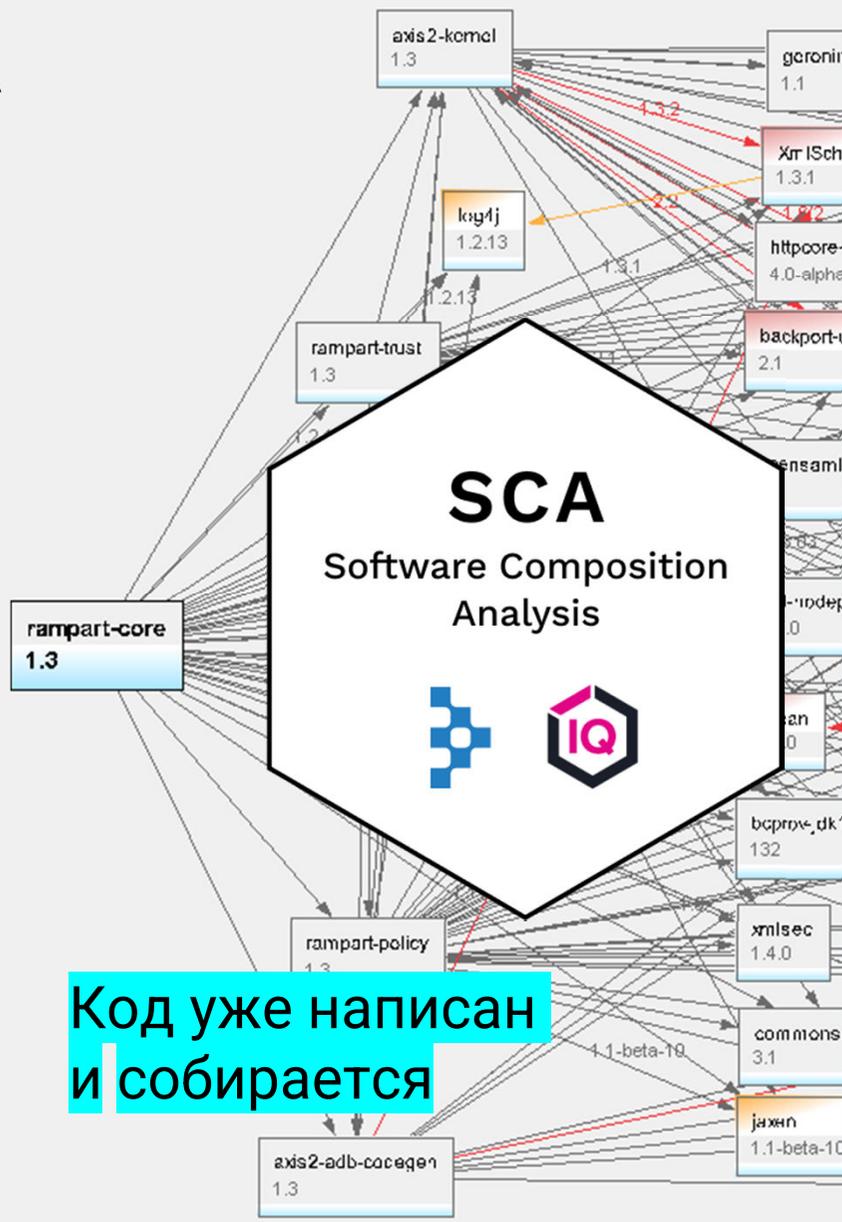


Серия региональных конференций с самым широким охватом ИБ-профессионалов

Код уже написан, собран и эксплуатируется



A



Код уже написан и собирается

Dashboard > Antiphish

Build History

trend v

Filter builds...

✓ #649	28 Sep 2022, 15:03
✓ #648	26 Sep 2022, 11:59
✓ #647	26 Sep 2022, 11:41
✓ #646	23 Sep 2022, 17:28
✓ #645	23 Sep 2022, 16:38
✓ #644	23 Sep 2022, 10:33
✓ #643	22 Sep 2022, 18:08
✗ #642	22 Sep 2022, 17:23
✓ #641	22 Sep 2022, 15:36
✓ #640	20 Sep 2022, 17:47

Atom feed for all Atom feed for failures

Stage View

Average stage times:
(Average full run time: ~4min)

Build #	Time	Commits	Checkout
#649	Sep 28 15:03	No Changes	52s
#648	Sep 26 11:59	No Changes	21s
#647	Sep 26 11:41	3 commits	59s
#646	Sep 23 17:28	1 commit	46s
#645	Sep 23 16:38	4 commits	54s
#644	Sep 23 10:33	2	47s

A Какие инструменты делают продукт безопасным?

```
246 if (Provider.class == roleTypeClass) {
247     Type providedType = ReflectionUtils.getLastTypeGenericArgument(dependencyD
248     2 Class providedClass = 1 ReflectionUtils.getTypeClass(providedType);
249
250     if (this.componentManager.hasComponent(providedType, dependencyDescriptor)
251         || 3 providedClass.isAssignableFrom(List.class) || providedClass.isA
```

A "NullPointerException" could be thrown; "providedClass" is nullable here.

Bug Major cert, cwe

```
252     continue;
253 }
```

RELIABILITY

0 Bugs **A**

SECURITY

0 Vulnerabilities **A** 1 Hotspots

MAINTAINABILITY

4 Code Smells 5 Debt min **A**

Quality Gate **Passed**
All conditions passed



Код уже написан

A Что такое Shift-Left Security?



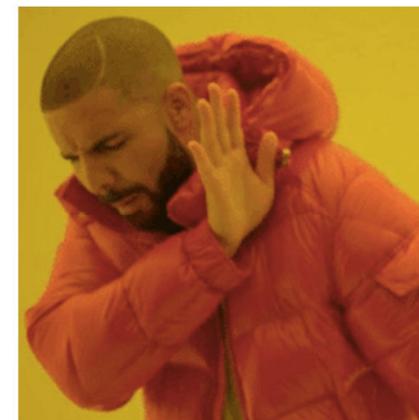
Планирование

Проектирование и дизайн

Реализация

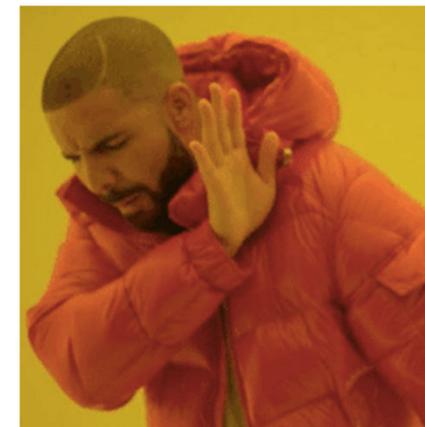
Тестирование

Эксплуатация



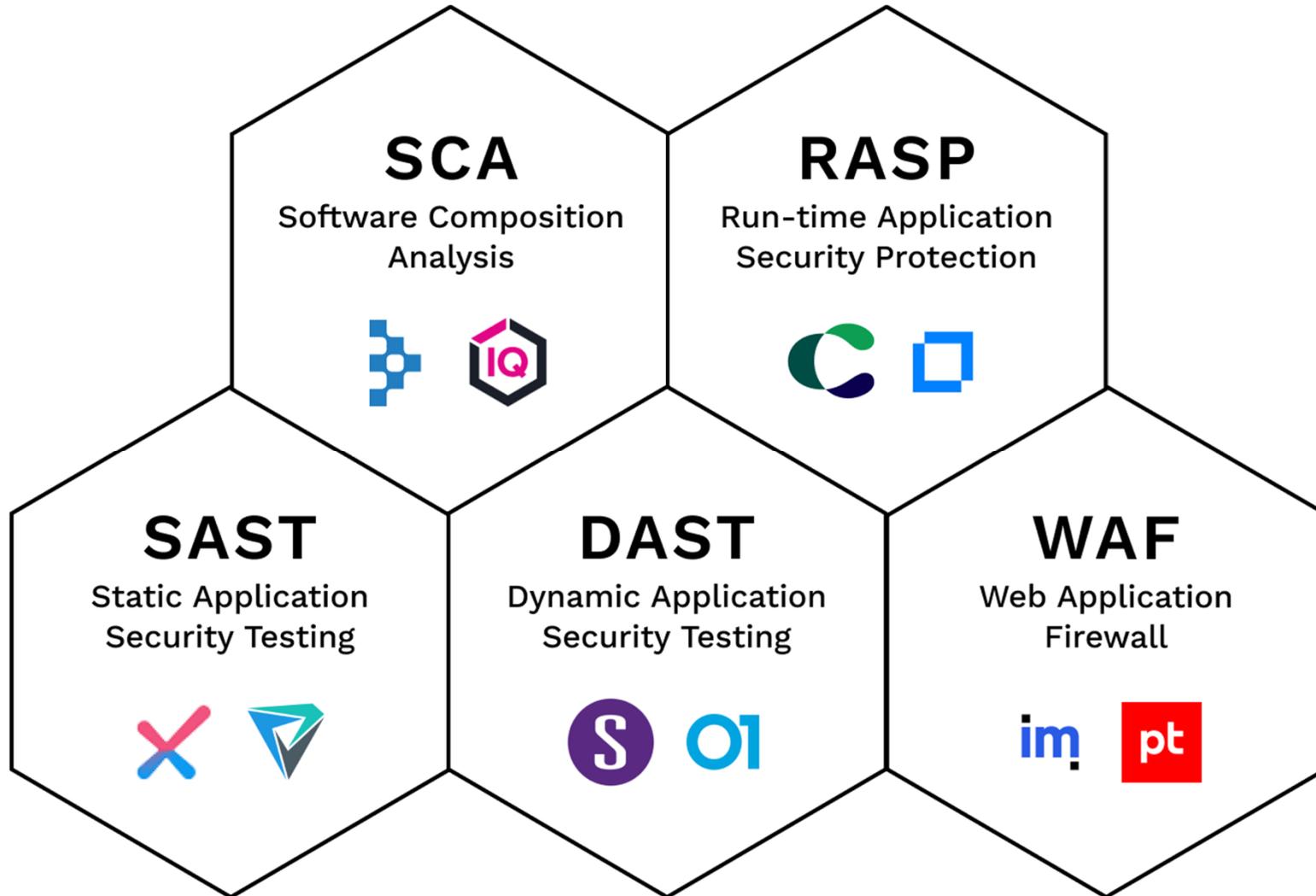
A

Относительная стоимость устранения дефектов ПО на разных этапах разработки

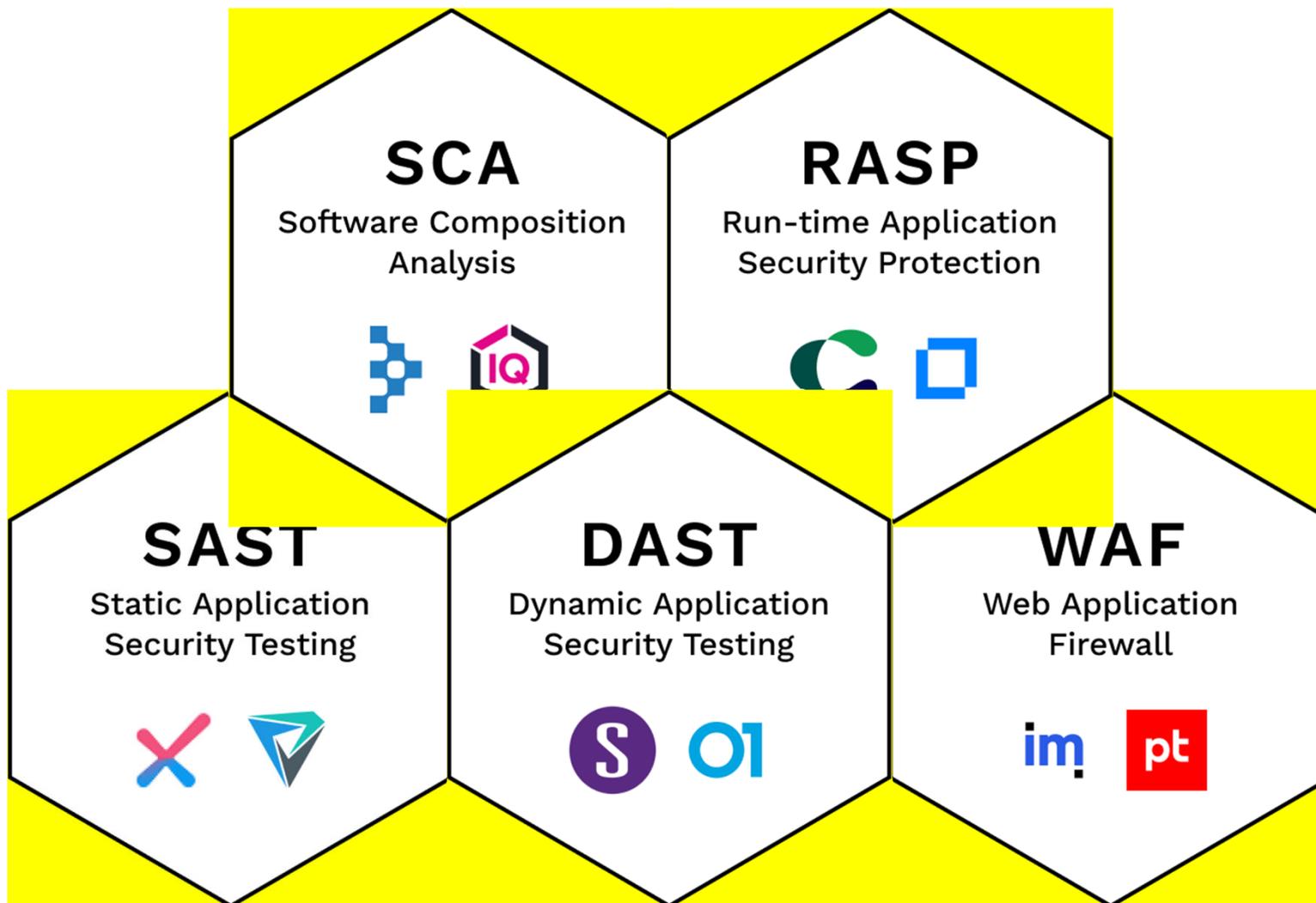


АНТИФИШИНГ

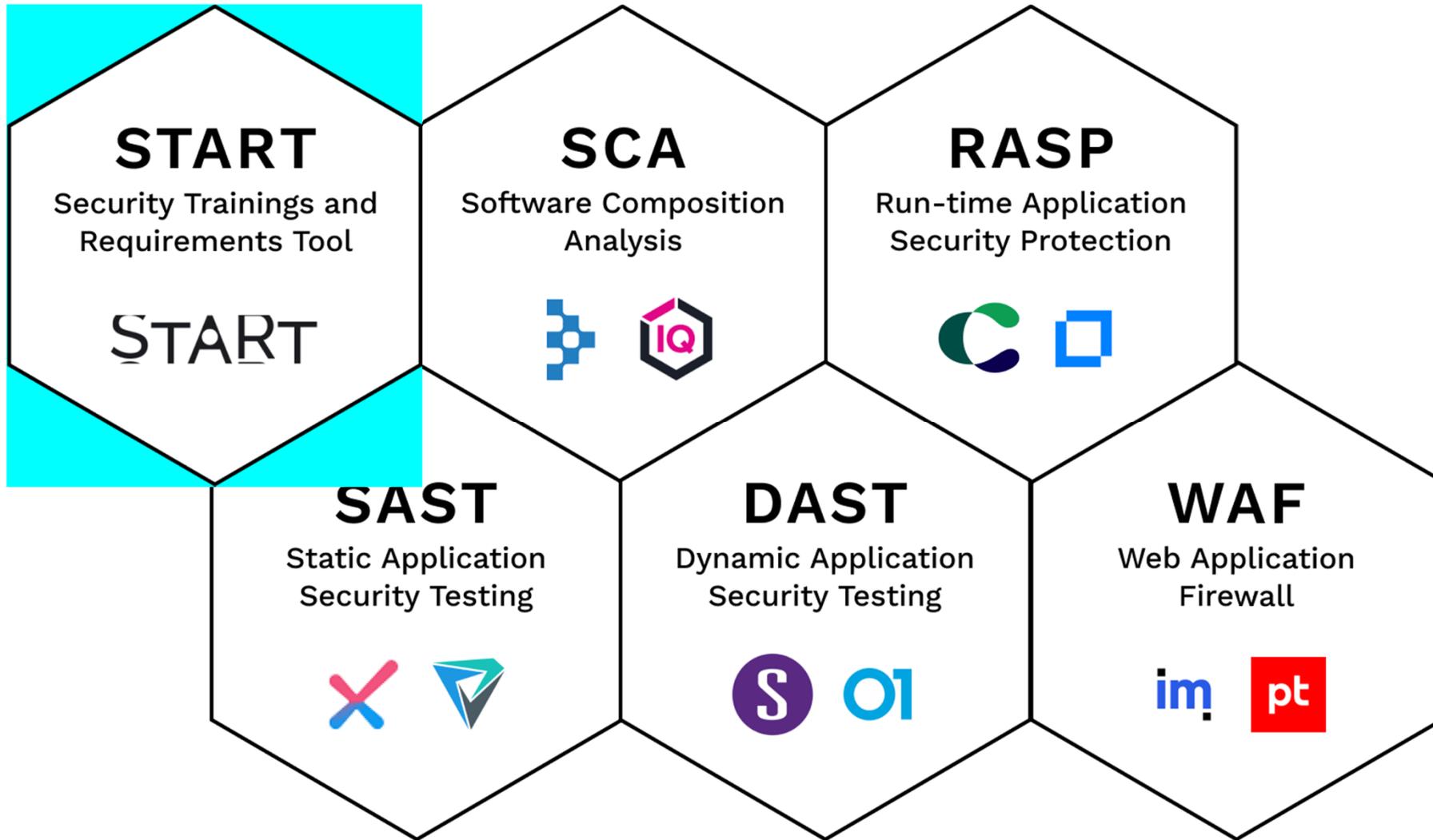
A Какие инструменты делают продукт безопасным?



A Инструменты не делают продукт безопасным



A Люди делают продукт безопасным



А Антифишинг. START для продуктовых команд

The screenshot displays the 'Anti-Fishing START' application interface. The main view is titled 'Мои проекты' (My Projects) and lists several projects with columns for 'Проект' (Project), 'Систем' (Systems), 'Требований' (Requirements), 'Последняя активность' (Last Activity), and 'Действия' (Actions). Projects listed include 'Модернизация ДБ0' (Modernization DB0), 'СЗ ПДн' (S3 PDn), and 'Тестовый проект' (Test project). Below the projects, there is a section for 'Коллекции требований' (Requirements Collections) featuring logos for 'Банк России' (Bank of Russia) and 'PCI Security Standards Council'.

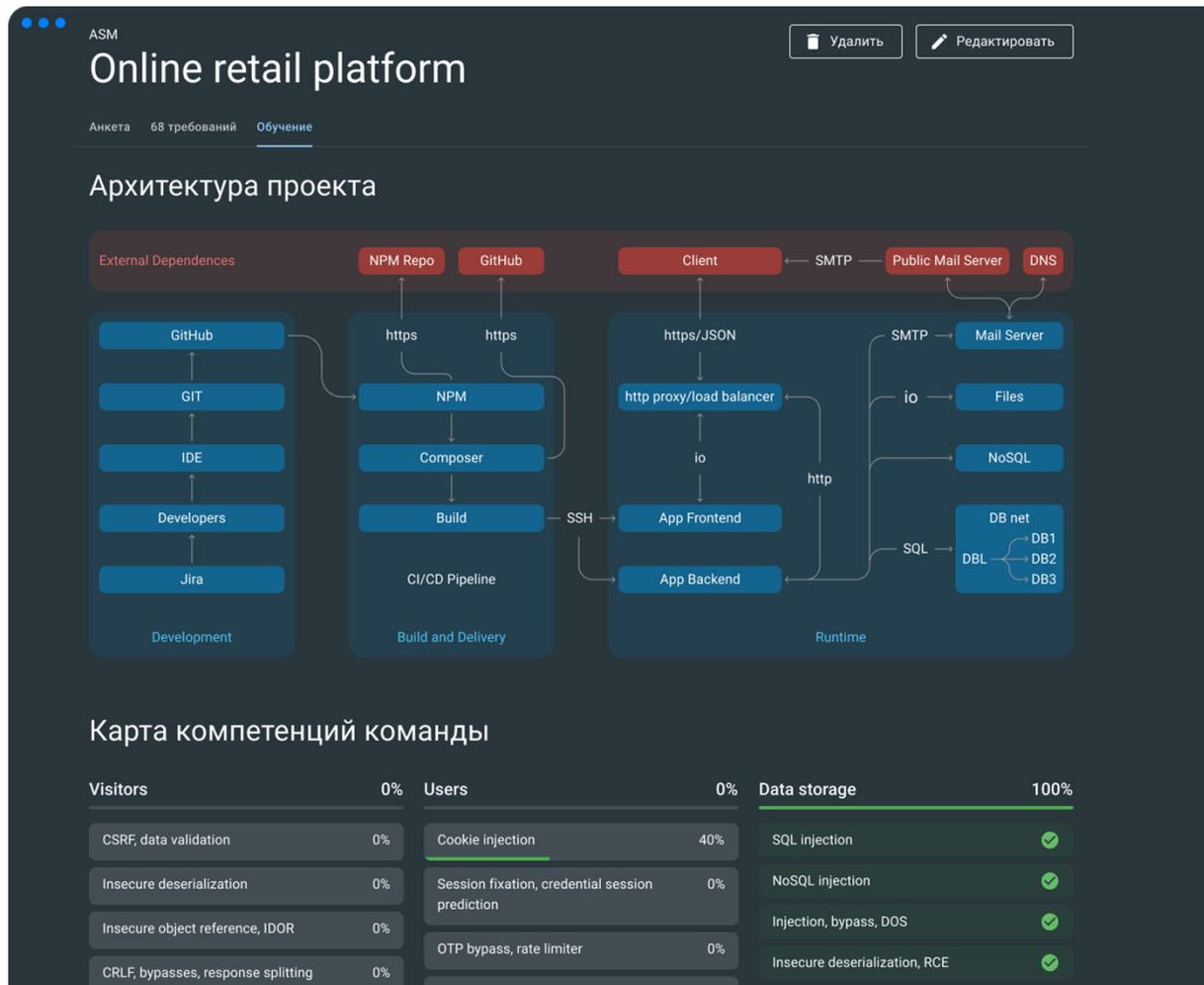
Overlaid on the screenshot is a document titled 'Приложение № 1 к Протоколу испытаний АС на соответствие требованиям по ИБ' (Appendix No. 1 to the Test Protocol for AS compliance with security requirements). The document contains a table with the following data:

№ п/п	Код	Формулировка требования	Результат испытания и замечания	Критичность	Срок устранения замечаний
1	AR	Архитектура и Дизайн			
2	AR3	Для взаимодействия с другими приложениями и компонентами должны использоваться учетные записи, обладающие минимально необходимыми полномочиями.	Без замечаний	Средняя	
3	CO	Техническое. Общие требования и документирование			
4	CO1	В документации на приложения должны быть перечислены все используемые криптографические библиотеки, цели и способы их	Без замечаний	Высокая	

Первое решение класса ASRTM (Application security requirements and threat management) на российском рынке.

Система для управления требованиями и знаниями по безопасности приложений, а также для обучения разработчиков ПО и продуктовых команд вопросам безопасной разработки.

А Антифишинг. START. EDU — интерактивный модуль обучения для продуктовых команд



Строит карту проекта

Назначает только актуальные обучающие модули

Доставляет знания и навыки прямо в Jira

START.EDU

Модуль интерактивного обучения команд актуальным вопросам безопасной разработки в рамках продукта Антифишинг.START.

Платформа за 15 минут выявит навыки разработчиков через тестирование и автоматически составит матрицу их компетенций.

Каждому разработчику подбирается обучающий курс, согласно навыкам и текущим проектам, в которых он задействован.

START

The screenshot shows a user profile for Alexey Rybakov, a Frontend Developer, with a score of 250 and a 'Novichok' (Beginner) status. The interface is divided into several sections:

- Системы (Systems):** A row of progress cards for 'CTF' (0/10), 'START' (2/10), and 'LMS'. A 'Show more' button is located below.
- Карта компетенций (Competency Map):** A search bar with the placeholder 'Название контекста или юнита' and a 'Показывать' (Show) button set to 'Все' (All).
- Visitors (0%):** A list of skills with associated scores and star icons:
 - CSRF, data validation: +100 ★
 - Insecure deserialization: +100 ★
 - Insecure object reference, IDOR: +100 ★
 - CRLF, bypasses, response splitting: +100 ★
 - Insufficient anti-automation: +100 ★
 - Insecure parsing and reference: +50 ★
 - XXE, xpath injection: +50 ★
- Users (11%):** A list of skills with associated scores and star icons:
 - Cookie injection: 45 ✓
 - Session fixation, credential session prediction: 45 ✓
 - OTP bypass, rate limiter: +50 ★
 - Insufficient authorization: +50 ★
 - Insecure password checks: +50 ★
 - Weak password recovery validation, host header injection: +50 ★
- Data st...:** A partially visible list of skills including 'SQL inj...', 'NoSQL', 'Injectio...', and 'Insecu...'.

START.EDU

Каждый курс состоит из юнитов с актуальной теорией, обязательными примерами из реальной среды и проверочными заданиями, которые основаны на кейсах уязвимых приложений и помогают закрепить и проверить полученные знания.

Интеграция с JIRA синхронизирует обучение с другими рабочими процессами.

START

злоумышленник не располагает этой информацией.

Предположим, что у нас есть веб-приложение, в котором сессии хранятся в cookie, а пользователи могут изменить свой адрес электронной почты с помощью следующей HTML-формы:

```
HTML-form
1  <html>
2    <body>
3      <form action="/user/email" method="POST">
4        <input type="email" name="email" value="" />
5        <input type="submit">
6      </form>
7    </body>
8  </html>
9
```

Если пользователь введет новый адрес в форму и нажмет «Сохранить», его браузер отправит POST-запрос, содержащий данные из формы:

```
HTML-form
1  POST **/user/email** HTTP/1.1
2  Host: example.com
3  Content-Type: application/x-www-form-urlencoded
4  Content-Length: 22
5  **Cookie: PHPSESSID=JKcciBhFZ0tTp1xh7QW2DigRqdUZknbC**
6
7  **email=user@example.com**
8
```

Проанализировав запрос, потенциальный злоумышленник обнаружит, что он соответствует условиям для проведения успешной CSRF-атаки:

1. Действие по изменению адреса электронной почты в учетной записи пользователя представляет интерес для злоумышленника:

Защита от подд
запросов: CSRF

Теория

- ☑ Зачем этот курс
- ☑ Что такое CSRF
- 📄 Как происходит
- 📄 Как защититься
- 📄 Частые вопросы

Квиз

Практика

А Антифишинг. START. CTF

The screenshot displays the HackMeBank mobile application interface. At the top, there is a navigation bar with the bank's name and menu items: "HackMeBank", "Для вас", "Наши продукты", "Контакты", and "Личный кабинет". Below this, a "Счет" (Account) header is visible. The main content area is split into two columns. The left column features a promotional banner for a "Мультивалютная электронная карта от HackMeBank" (Multi-currency electronic card from HackMeBank), highlighting a 87.3% cashback and a monthly interest rate on the balance. Below the banner is a "Оформить карту" (Apply for card) button. The right column shows account actions: "Пополнить" (Top up), "Заблокировать" (Block), "Перевыпустить" (Re-issue), and "Поменять пароль" (Change password). Below these is a "Последние операций" (Recent transactions) section for December 25, 2021, listing several debit transactions from various merchants like KAFE OTDУKH, Перекресток, and Burger King. At the bottom, there is a section titled "О карте" (About the card) with three key features: "Бесплатный выпуск" (Free issuance), "Высокий кэшбэк" (High cashback), and "Кредитный лимит" (Credit limit).

Тренажер в формате действующего интернет-банка

О карте

- Бесплатный выпуск**
бесплатное обслуживание при выполнении условий
- Высокий кэшбэк**
получай до 87.3% за покупки у партнеров сервиса
- Кредитный лимит**
добавляйте при необходимости кредитный счёт до 1 000 000 рублей

Дата	Списание	Сумма	Категория
25 декабря 2021	с Дебетовая *8149 KAFE OTDУKH	-235,00 Р	Фастфуд
	с Дебетовая *8149 Перекресток	-80,20 Р	Продукты
	с Дебетовая *8149 Магазин продуктов	-9 580,36 Р	Продукты
	с Дебетовая *8149 Оплата на PayPal	-1 528,14 Р	Переводы
	с Дебетовая *8149 Burger King	-623,92 Р	Фастфуд
	с Дебетовая *8149 Покупка пакета объявлений	-1 783,25 Р	Сервисы
	с Дебетовая *8149	-1 518,00 Р	

Тренажер **по практической безопасности** в рамках Антифишинг. START.

START



Как вести безопасную разработку и создавать защищённые продукты

Используйте наши рекомендации, чтобы ваши процессы и продукты соответствовали лучшим практикам безопасной разработки

antiphish.ru/products/start

devsecops@antiphish.ru

Шаги по разработке защищенного продукта

1



Создайте собственный каталог требований

5

Используйте CI-системы правильно

9

Проводите ручное тестирование

2

Используйте инструменты обеспечения безопасности

6

Примените статический анализ кода

10

Проводите внутренние пентесты



4

4

Делайте качественный код-ревью

8

Делайте автотесты и динамический анализ

Повышайте квалификацию разработчиков



Повышайте квалификацию разработчиков

А Продукты «Антифишинга» уже используют



М.ВидеоЭльдорадо





www.antiphish.ru
ask@antiphish.ru



КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

antiphish.ru/products/start