

Start X

Как вести безопасную разработку и создавать защищённые продукты

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

<https://startx.team/products>

ask@startx.team

Шаги по разработке защищенного продукта

1



Создайте собственный каталог требований

2

Используйте модель обеспечения безопасности ПО OWASP

3

Пишите безопасный код

4

Делайте качественный код-ревью

5

Используйте CI-системы правильно

6

Применяйте статический анализатор

7

Проверяйте собственное тестовое окружение

8

Делайте автотесты и динамический анализ

9

Проводите ручное тестирование

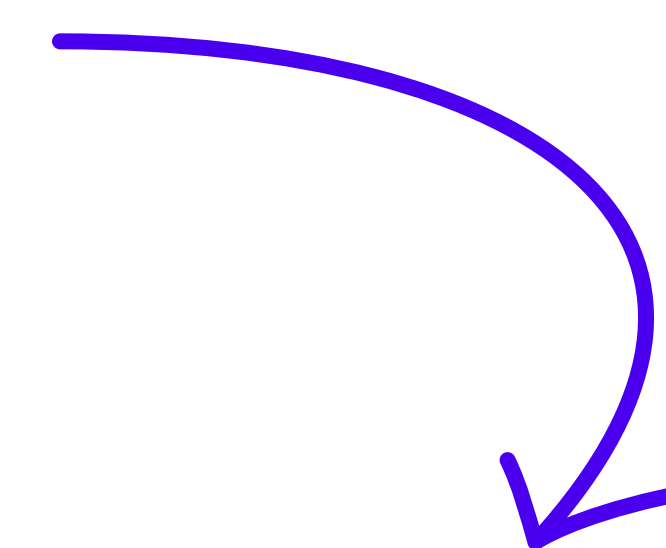
10

Проводите внутренние пентесты

11



Повышайте квалификацию разработчиков



Создайте собственный каталог требований

1

Включите туда:

- а) требования разработки защищенного ПО на начальных этапах создания ПО;
- б) стандарты на используемые ОС, СУБД, сервера приложений и требования к их безопасной настройке;
- в) стандартизованные процессы верификации требований до перевода релизов в продуктивную среду;
- г) руководство для разработчиков;
- д) отслеживание лучших практик и опыт OWASP Top 10.

Система для управления требованиями

Start REQ

Маркетплейс OST

Личный кабинет поставщика

Анкета

Требования (66)

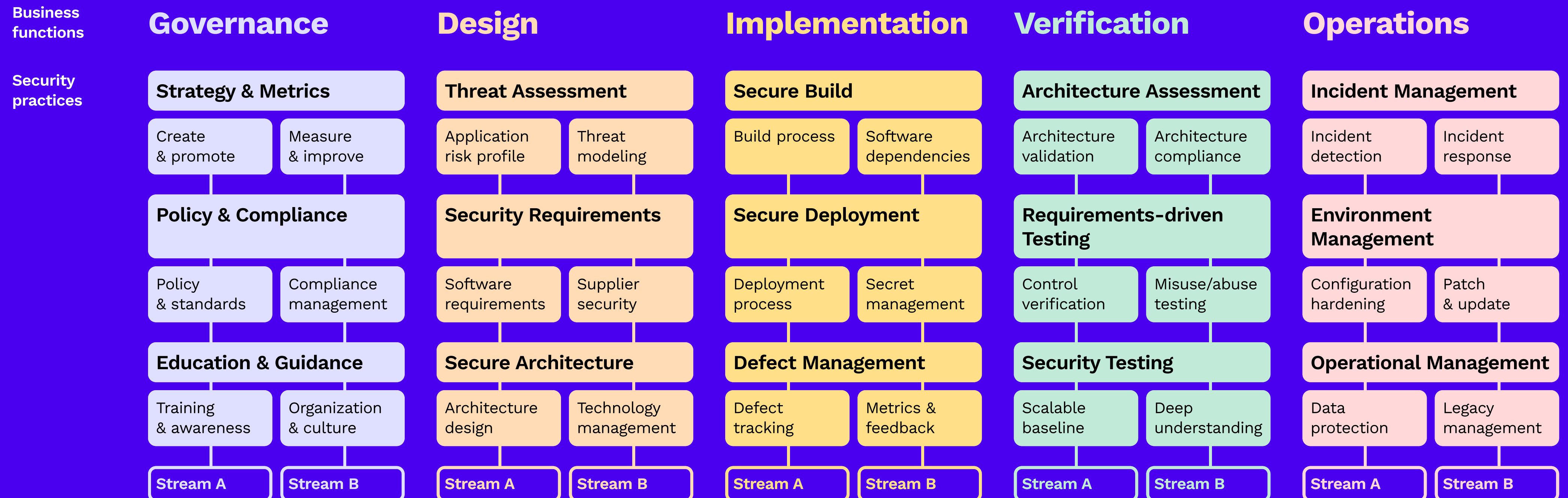
+ Добавить Требование

Отчёты

<input type="checkbox"/>	Категория	Короткое название	Описание	Статус реализации	Результат тестирования	Тип требования
<input type="checkbox"/>	Технические. Идентификация и аутентификация	AU1	Все интерфейсы и ресурсы приложения должны быть доступны только после успешного прохождения аутентификации (за исключением общедоступных ресурсов для приложений, с доступом только из защищенного периметра)	<input type="text"/>	Некритичное замечание	
<input type="checkbox"/>	Архитектура и Дизайн	AR13	ar13	<input type="text"/>	Критичное замечание	

Используйте модель обеспечения безопасности ПО OWASP

2



Пишите безопасный код

3

- А. Разделяйте функционал по версиям.
- Б. Поддерживайте регулярное обновление кода в соответствии с новыми исправлениями.
- В. Используйте GIT для хранения кода.
- Г. Любые изменения в коде заносите в журнал, на них можно всегда откатиться.
- Д. Ведите лог по тому, кто что сделал и когда.
- Е. Проводите анализ безопасности используемых в продуктах компании сторонних библиотек и компонентов.

Пример разделения функционала по версиям

The screenshot displays the Bitbucket interface for a repository named 'Antiphish YII'. The left sidebar contains navigation options: Source, Commits, Branches (highlighted), Pull requests, Pipelines, Deployments, Jira issues, Security, Downloads, and Repository settings. The main content area shows the 'Branches' page with a search bar containing 'release/2.4.6'. Below the search bar, there are filters for 'Active branches' and 'Branch type'. A table lists the branches with columns for Branch, Behind, Ahead, Updated, Pull request, Builds, and Actions.

Branch	Behind	Ahead	Updated	Pull request	Builds	Actions
master MAIN PRODUCTION			KR 5 days ago			...
release/2.4.6-cu9.2	867	3	RF 2022-04-06	Create		...
release/2.4.6-cu9.1	867	4	2022-04-06	Create		...
release/2.4.6-cu6.1	1159	7	2022-02-22	Create		...
release/2.4.6-cu3	1261	1	2022-02-01	Create		...

Делайте качественный код-ревью

4

- А. Код всегда пишете в отдельной ветке. Затем разработчик создает pull-request, который попадает на код-ревью и только потом такой код попадает в другие ветки, в том числе в релизную.
- Б. Код-ревью проводят минимум 2 разработчика. Ревьюером не может быть разработчик, который написал этот код.
- В. Проводите security код-ревью — поиск уязвимостей путем анализа исходного кода.

Пример код-ревью

```
learning / certificates / CertificatesService.php

@@ -10,11 +10,11 @@ class CertificatesService extends Component
    public const CODE_FILE_UPLOAD_ERROR = 1;
    /** @var string */
-   public $certificatesStorePath;
    public function init()
    {
-       $this->certificatesStorePath = \Yii::getAlias('@app/certs');
        parent::init();
    }

@@ -33,11 +33,19 @@ class CertificatesService extends Component
    }
-   public function saveFile(UploadedFile $file, string $name) {
-       $new_name = substr(md5($name), 0, 8) . '.' . $file->extension;
-       $path = \Yii::getAlias('@app/certs/' . $new_name);
-       if (!$file->saveAs($path)) {
-           return $new_name;
-       }
-   }
+   /**
+    * @param UploadedFile $file
+    * @param string $name
+    * @return string
+    * @throws Exception
+    */
+   public function saveFile(UploadedFile $file, string $name): string
+   {
+       $new_name = substr(md5($name), 0, 8) . '.' . $file->extension;
+       $path = \Yii::getAlias('@app/certs/' . $new_name);
+       if (!$file->saveAs($path)) {
+           return $new_name;
+       }
+   }
}
```


Используйте CI-системы правильно

При каждом коммите CI делает сборку продукта с нуля и развертывает ее на тестовом сервере. Далее запускает набор автотестов, которые реализуют статический анализ кода, проверку на уязвимости во внешних библиотеках, динамический анализ собранного приложения.

5

The screenshot displays a CI dashboard for a project named 'Antiphish'. The 'Build History' section lists recent builds with their IDs, dates, and times. Build #642 is marked as failed, while others are successful. The 'Stage View' section provides a detailed look at the build process, showing average stage times and full run times for each build. A progress bar indicates the current stage's progress.

Dashboard > Antiphish

Build History trend

Filter builds...

Build ID	Date and Time	Status
#649	28 Sep 2022, 15:03	Success
#648	26 Sep 2022, 11:59	Success
#647	26 Sep 2022, 11:41	Success
#646	23 Sep 2022, 17:28	Success
#645	23 Sep 2022, 16:38	Success
#644	23 Sep 2022, 10:33	Success
#643	22 Sep 2022, 18:08	Success
#642	22 Sep 2022, 17:23	Failure
#641	22 Sep 2022, 15:36	Success
#640	20 Sep 2022, 17:47	Success

Atom feed for all Atom feed for failures

Stage View

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

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

Checkout 52s

Применяйте статический анализатор

6

- А. Интегрируйте статический анализатор в процессы системы CI и запускайте при любом коммите в репозиторий.
- Б. Результат: отчет с рекомендациями по улучшению кода и вердикт — можно ли текущий реквест, коммит или ветку мержить в основную ветку в GIT.

Пример работы статического анализатора

```
246 if (Provider.class == roleTypeClass) {  
247     Type providedType = ReflectionUtils.getLastTypeGenericArgument(dependencyDe  
248     2 Class providedClass = 1 ReflectionUtils.getTypeClass(providedType);  
249  
250     if (this.componentManager.hasComponent(providedType, dependencyDescriptor.g  
251         || 3 providedClass.isAssignableFrom(List.class) || providedClass.isA  
  
252         continue;  
253     }
```

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

 Bug  Major

 cert, cwe

RELIABILITY

 0  A
Bugs

Quality Gate
Passed
All conditions passed

SECURITY

 0  A
Vulnerabilities

 1
Hotspots

MAINTAINABILITY

 4
Code Smells

 5  A
min Debt

Проверяйте собственное тестовое окружение

7

- А. Сделайте набор тестовых серверов в собственной инфраструктуре. А также для внутреннего тестирования применяйте полную копию серверов, используемых заказчиками с примененными стандартами по их безопасной настройке, и их особенностями инфраструктуры. Любое обновление on-premise заказчикам сопровождайте предварительным регрессионным тестированием на аналогичном тестовом контуре, развернутом в вашей инфраструктуре.
- Б. Храните зашифрованные резервные копии на нескольких независимых площадках.

Пример тестового окружения в Jenkins

The screenshot shows the Jenkins web interface. At the top left is the Jenkins logo. To its right is a search bar with the text 'Search (⌘+K)' and a help icon. Further right is the user name 'Павел Горх' with a dropdown arrow and a 'log out' button. Below the top bar is a breadcrumb trail: 'Dashboard > Antiphish > QA_Environments >'. On the left side, there is a sidebar menu with items: 'Status' (selected), 'Configure', 'New Item', 'People', 'Build History', 'Project Relationship', 'Check File Fingerprint', 'Move', and 'Open Blue Ocean'. The main content area shows a folder icon and the name 'QA_Environments'. Below this, there is a filter button 'All' and a plus sign. To the right of the folder name is an 'Add description' link with a pencil icon. Below these elements is a table with the following columns: 'S', 'W', 'Name ↓', 'Last Success', 'Last Failure', 'Last Duration', 'Fav', and '# Issues'. The table contains three rows of data:

S	W	Name ↓	Last Success	Last Failure	Last Duration	Fav	# Issues
Folder icon	Cloud icon	aleksey.antph.ru	N/A	N/A	N/A	Star icon	-
Folder icon	Cloud icon	auto.antph.local	N/A	N/A	N/A	Star icon	-
Folder icon	Cloud icon	develop.antph.local	N/A	N/A	N/A	Star icon	-

Делайте автотесты и динамический анализ

Настройте автоматизированный запуск автотестов после каждой сборки кода системой CI. По итогу генерируется отчет с результатами прохождения автотестов, что дает время разработчикам оперативно исправлять ошибки.

8

The screenshot displays a web-based test runner interface. At the top, it shows the project name 'antiphish' and the section 'Launches'. A progress bar on the right indicates 16 tests. Below this, there are tabs for 'Overview', 'Tree', and 'Errors', with 'Tree' selected. The main area is titled 'Test results' and contains a table of test items. The table has columns for 'Id', 'Name', and 'Status'. The first row is highlighted, showing a passed test with ID '#805' and name 'Add new certificate local...'. To the right of the table, there is a detailed view for the selected test, including tabs for 'Overview', 'History', 'Retries', and 'Attachments'. The 'Description' section shows 'No description', and the 'Precondition' section shows 'No precondition'. The 'Execution' section shows a sequence of four steps: 1. Create random certificate in manage, 2. Add new locale to created course, 3. Check certificate response, and 4. Check that certificate is displayed in certs l... Below this, there is another execution block with one step: 1. afterClass.

Id	Name	Status
#805	Add new certificate local...	PASSED
#218	Add new course loc...	PASSED
#1043	All failed attempts	FAILED
#1039	All targets are disp...	FAILED
#40	Assign target on ra...	PASSED
#1044	Attempts not displ...	FAILED
#281	Auth with created c...	PASSED
#282	Auth with created c...	PASSED
#283	Auth with created c...	PASSED
#288	Auth with created c...	PASSED
#289	Auth with created c...	PASSED
#250	Auth with existing c...	PASSED
#315	Auto select course	PENDING
#25	Cancel education c...	PASSED
#44	Cancel education c...	PASSED

Проводите ручное тестирование

- А. Проверьте функционал командой тестирования.
- Б. Проводите регрессы, смоук тесты перед выпуском обновлений системы.

9

The screenshot displays a test management application interface. On the left is a dark sidebar with various icons for navigation. The main area is divided into two panels. The left panel shows a list of test cases under the heading 'Test cases'. The right panel shows the details for test case #401, including its description, preconditions, and a scenario.

Test cases (Total test cases: 666)

Id	Name	Status	Created date
#371	Add client to license group - alternative and negative	REVIEW	
#372	Add client to license group - main positive	REVIEW	
#548	Add Department - alternative and negative		
#545	Add Department - Main positive		
#504	Add LDAP profile - "Alternative and negative"		
#517	Add LDAP-profile "main positive"		
#805	Add new certificate localization	ACTIVE	
#218	Add new course localization	ACTIVE	
#401	Add preview to courses "alternative and negative"		

#401 Add preview to courses

Overview History Attachments Mut

Description

Preconditions:

1. At least one <Client> existing in system
2. At least one <target> existing in system
3. At least one <course> without preview
4. There is at least one <Gif> on PC
5. There is at least one <image.jpeg> on PC

Precondition

No precondition

Scenario

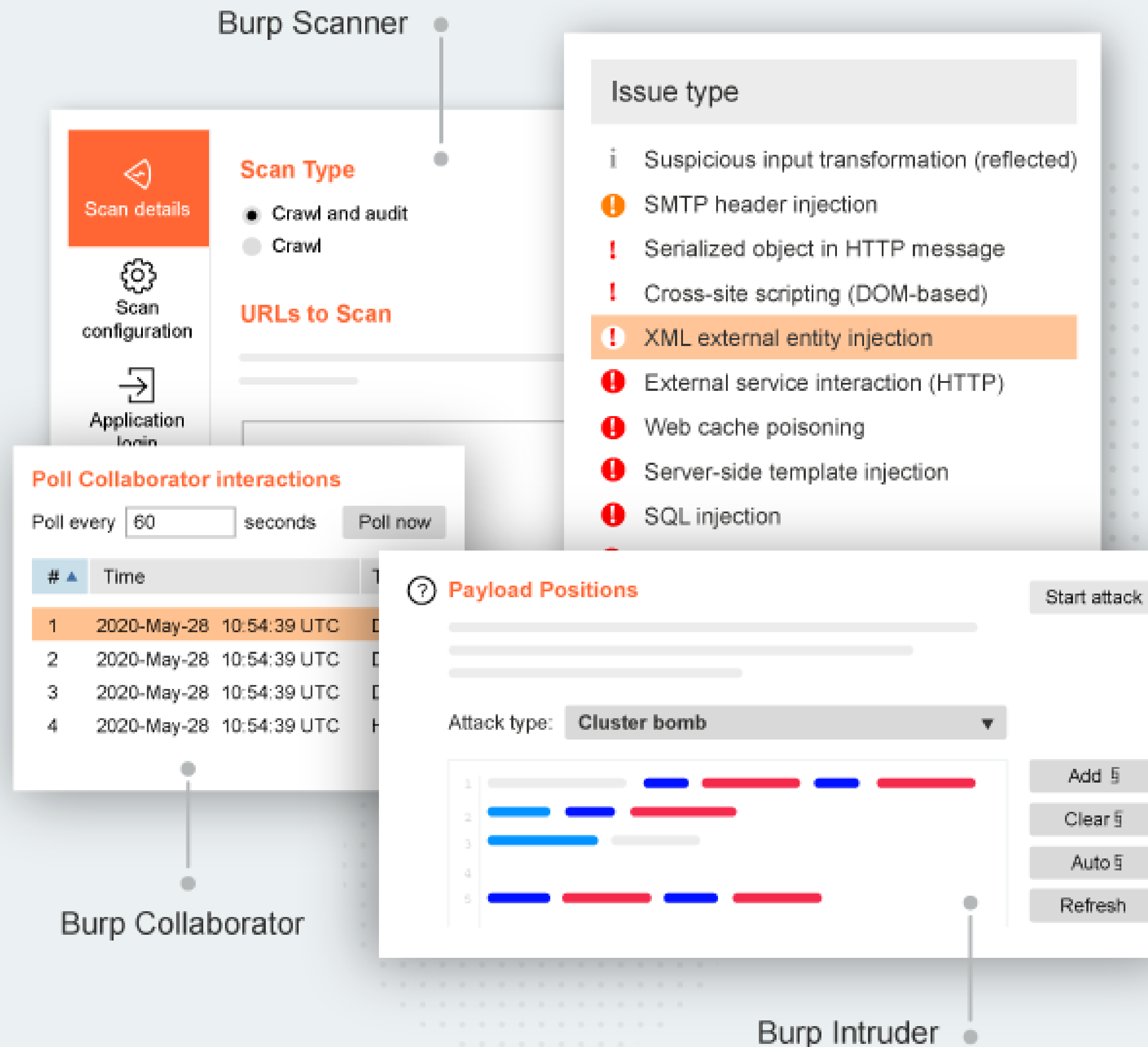
- 1 Login in Antiphishing and go to user settings
 - 1.1 Login successful
 - 1.2 Settings are opened
- 2 In section 'Курсы Антифишинг' open 'Add new course' button
 - 2.1 Pop-up for editing course is opened
- 3 Press link 'Превью' and select <Gif> Hover over the <Gif>

Проводите внутренние пентесты

Раз в квартал проводите ручной пентест, в том числе с использованием автоматизированных инструментов:

- а) Burp Suite Pro,
- б) OWASP ZAP,
- в) w3af и других.

10



Повышайте квалификацию разработчиков

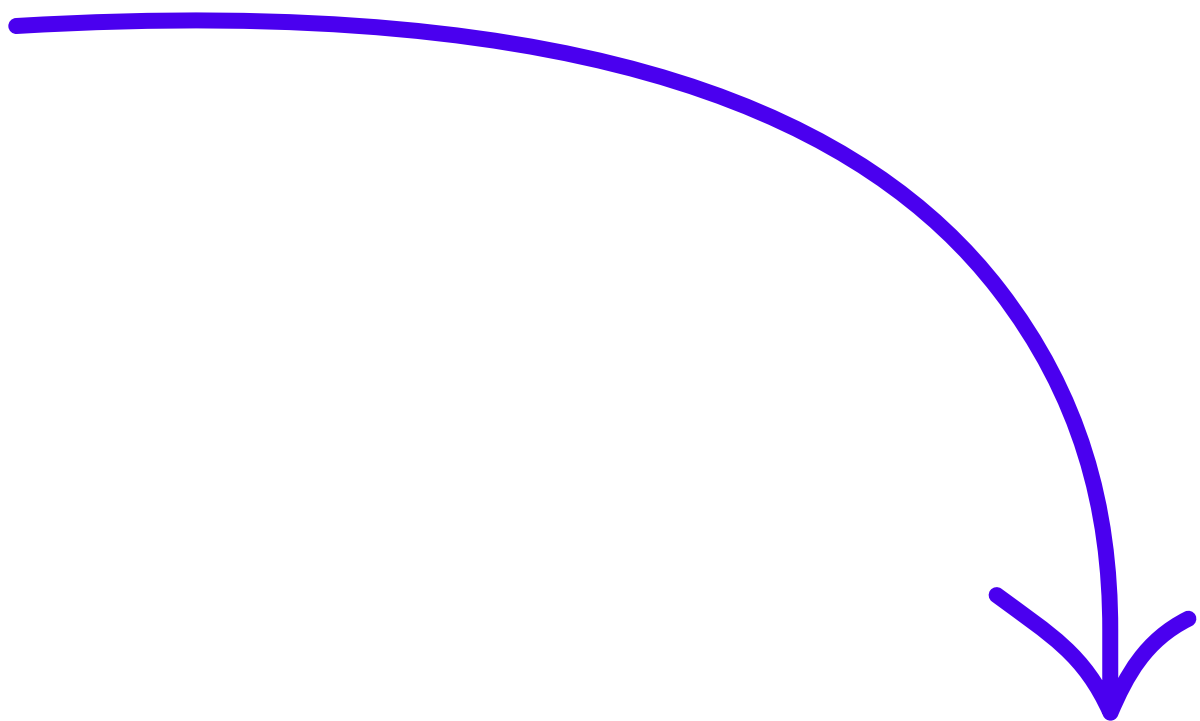
11

Проводите:

- а) ретроспективу выявленных в ходе security ревью недостатков;
- б) мастер-классы по безопасной разработке;
- в) внутренние курсы по архитектурным принципам создания защищенных продуктов и практикам создания безопасных приложений.

Принимайте участие в конференциях по практической безопасности, например: Positive Hack Days, Zeronights.

Если вы хотите, чтобы ваша команда:

- ☑ реализовывала все необходимые требования по ИБ,
 - ☑ применяла лучшие практики по безопасной разработке,
 - ☑ как результат — выпускала защищенные продукты
- 

**Попробуйте продукты Start X
для разработчиков**

Start REQ – первое решение класса ASRTM, Application Security Requirements and Threat Management, на российском рынке

Start X

The image displays the Start REQ application interface, which is a web-based tool for managing security requirements and threats. The interface is shown in a dark theme and includes a sidebar with navigation options: Admin, Проекты, Системы, Настройки, and Выйти. The main content area is titled "Мои проекты" and lists several projects, including "Модернизация ДБО" and "СЗ ПДн". A table below the projects lists the number of systems and requirements for each. The interface also features a "Добавить Проект" button and a "Добавить Требование" button. In the bottom right corner, a document titled "Приложение № 1 к Протоколу испытаний АС на соответствие требованиям по ИБ" is displayed, containing a table with columns for "№ п/п", "Код", "Формулировка требования", "Результат испытания и замечания", "Критичность", and "Срок устранения замечаний". The document also includes logos for "Банк России" and "PCI Security Standards Council".

№ 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	Технические. Общие требования и документирование			

Start EDU

Платформа по обучению продуктовых команд навыкам безопасной разработки.

Для владельцев продуктов, AppSec-специалистов, тимлидов, разработчиков и других членов продуктовых команд. На конкретных рабочих ситуациях и контекстах объясняет, как реализовать выставленные требования по безопасности в разрабатываемом ПО.

Start X

Алексей Рыбаков
Фронтенд-разработчик

250
Новичок

Системы

- CTF: Пршел 0/10
- START: Пршел 2/10
- LMS H: Прше.

Show more ▾

Карта компетенций

Название контекста или юнита | Показывать Все

Visitors	0%	Users	11%	Data sto
CSRF, data validation	+100 ★	Cookie injection	45 ✓	SQL inj
Insecure deserialization	+100 ★	Session fixation, credential session prediction	45 ✓	NoSQL
Insecure object reference, IDOR	+100 ★	OTP bypass, rate limiter	+50 ★	Injection
CRLF, bypasses, response splitting	+100 ★	Insufficient authorization	+50 ★	Insecur
Insufficient anti-automation	+100 ★	Insecure password checks	+50 ★	
Insecure parsing and reference	+50 ★	Weak password recovery validation, host header injection	+50 ★	
XXE, xpath injection	+50 ★			

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 X

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 подделке запросов: CSRF

Теория

✓ Зачем этот курс

✓ Что такое CSRF

📖 Как происходит

📖 Как защититься

📖 Частые вопросы

Квиз

Практика

Для проведения демонстрации

Напишите нам на ask@startx.team

Start X

