

PT Application Inspector 4.4

Новые возможности для командной разработки

Спикеры



**Владислав
Феофилактов**

Программист,
Группа разработки средств
интеграции



**Андрей
Лядусов**

Руководитель группы
разработки средств
интеграции



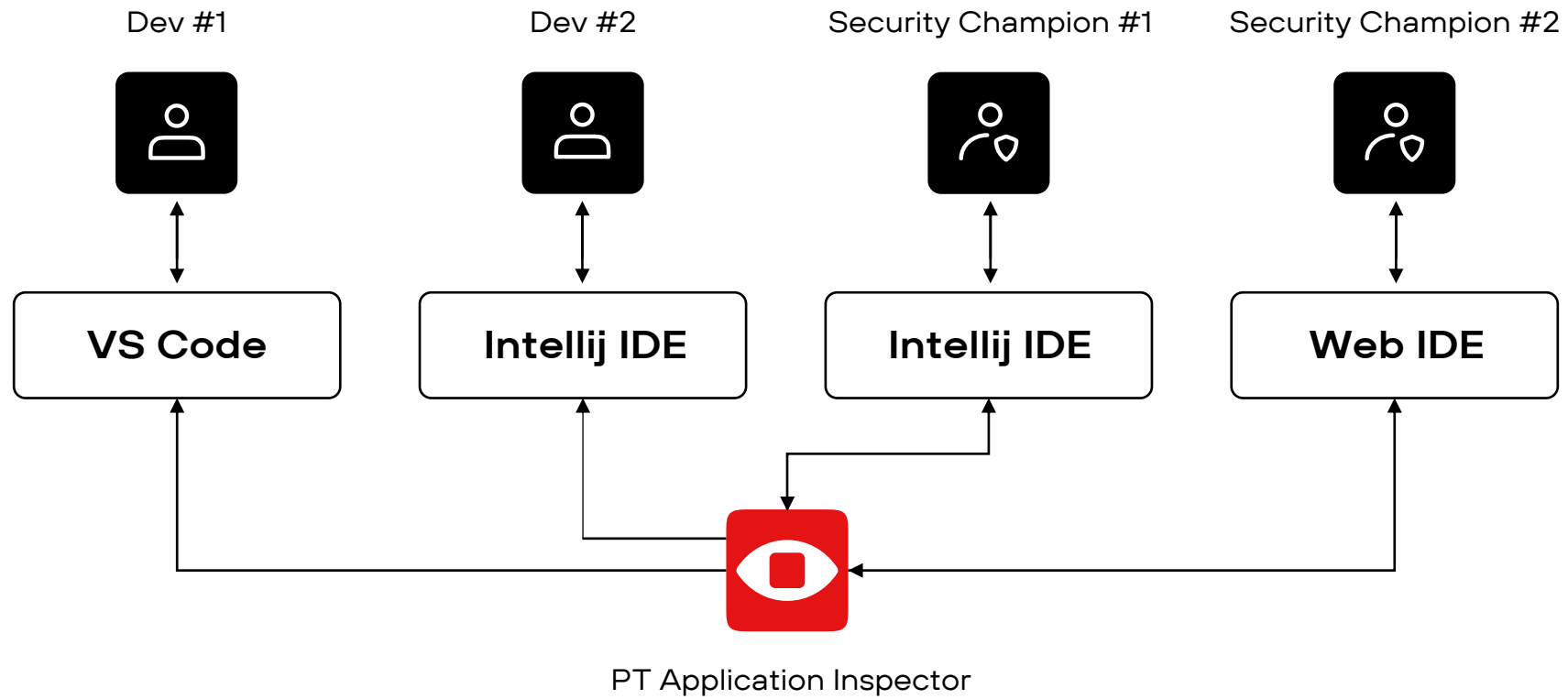
**Даниил
Бакин**

Программист,
Группа разработки средств
интеграции

План вебинара

- Зачем нужна командная работа
- Демонстрация интеграции Application Inspector Enterprise и IDE-плагинов
- Web IDE
- Ответы на вопросы

Концепция



```
[PT AI] DATA FLOW pinned ✓ ✕ ◀ ▶ ⚙
SQL Injection
./cubrid_execute.php ★ Best place to fix Discard
3 $sql = "SELECT g.event_code, e...

./cubrid_execute.php Entry point
1 <?php

./cubrid_execute.php Data entry point
3 $sql = "SELECT g.event_code, e...
```

Я доверял тебе

Ролевая модель



Администратор



Разработчик



Аудитор



Менеджер безопасности

Как работает синхронизация статусов

```
php cubrid_execute.php
1  <?php
2  $conn = cubrid_connect("localhost", 33000, "demodb");
3  $sql = "SELECT g.event_code, e.name FROM " . $_GET['a'];
4  $req = cubrid_execute($conn, $sql);
5  $req = cubrid_execute($conn, $sql, CUBRID_ASYNC);
6  ?>
```

OUTPUT PROBLEMS 151 TERMINAL DEBUG CONSOLE [PT AI] SCAN HISTORY

▼ php cubrid_execute.php 3

- ⊗ [Confirmed] SQL Injection PT Application Inspector [Ln 4, Col 1]
- ⊗ [Confirmed] SQL Injection PT Application Inspector [Ln 5, Col 1]

Локальная работа через IDE

Уязвимость	Уязвимый файл	Идентификатор ▼
▼ ./cubrid_execute.php : 3 2		
• ■ \$req = cubri...	./cubrid_execute.php : 5	76 ✓
Внедрение SQ...		
• ■ \$req = cubri...	./cubrid_execute.php : 4	75 ✓
Внедрение SQ...		

Application Inspector Enterprise

Hash (Положение уязвимости + Тип уязвимости +
Содержимое уязвимого кода + Эксплоит + ...)

Демонстрация VS Code

Демонстрация IntelliJ Idea

Web IDE

The screenshot displays a web IDE with a central editor showing PHP code for a login form. The code includes fields for username and password, a submit button, and a success message. A security tool has identified several vulnerabilities, including Cross-Site Scripting (CSP) and SQL Injection. The 'PROBLEMS' panel on the right lists these issues with their locations in the code.

```
43 <p><?php echo $sSuccessMsg;?</p>
44 <p>Username: <input type="text" name="username" id="username
45 <p>Password: <input type="password" name="passwd" id="passwd
46 <p><input type="submit" class="small button" name="submit" i
47 </fieldset>
48 </form>
49 </div><br/><br/><br/>
50 <center>
51 <?php
52 if($showhint === true && isset($sql)) {
53 echo '<div class="eight columns centered"><div class="alert-
54 echo $sql;
55 echo '<a href="" class="close">&times;</a></div></div>';
56
57 >
58 </center>
59 </div>
60
61 <!-- Included JS Files (Uncompressed) -->
62 <!--
63
64 <script src="../../javascripts/jquery.js"></script>
65
```

PROBLEMS (43)

- [Confirmed] Cross-Site Scripting PT Application Inspector [Ln 57, Col 1]
- Index.php Sources • login-5 (2)
 - [Confirmed] SQL Injection PT Application Inspector [Ln 8, Col 3]
 - [Confirmed] Cross-Site Scripting PT Application Inspector [Ln 54, Col 5]
- Index.php Sources • login-6 (1)
 - [Confirmed] SQL Injection PT Application Inspector [Ln 11, Col 1]
- index.php Sources • upload-3 (4)
 - [Confirmed] Arbitrary File Modification PT Application Inspector [Ln 35, Col 7]
 - [Confirmed] Unrestricted File Upload PT Application Inspector [Ln 35, Col 7]
 - [Discarded] Arbitrary File Creation PT Application Inspector [Ln 35, Col 7]
 - [Confirmed] Cross-Site Scripting PT Application Inspector [Ln 36, Col 8]
- config.php Sources • config (1)



Даниил Бакин

Как работает Web IDE?

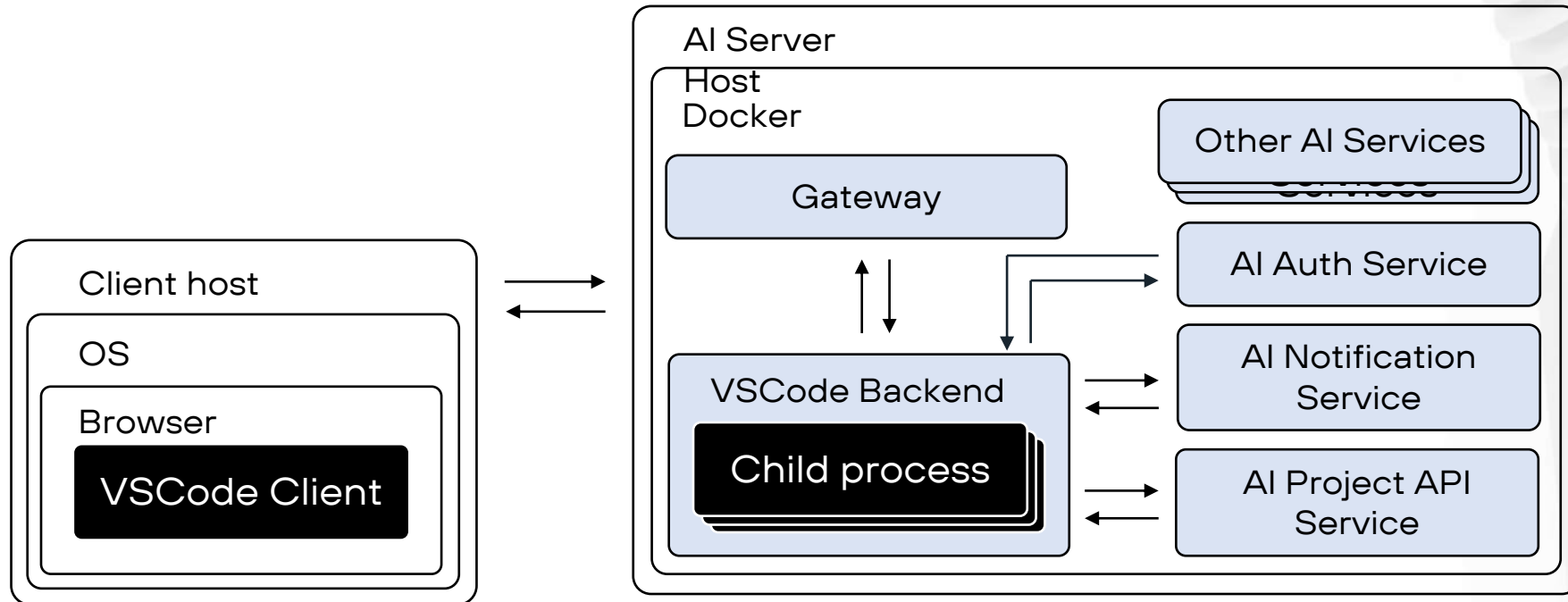


Диаграмма взаимодействия модуля Web IDE с другими сервисами PT Application Inspector

Демонстрация Web IDE

Где можно попробовать?



Application Inspector



Visual Studio Code



IntelliJ IDEA

Спасибо!