Блок PHP. Отчет о защите приложения

В рамках данной работы, было необходимо защитить приложение от SQL-инъекций и XSS-атак.

SQL-инъкции

Для защиты от данного рода уязвимостей используется PDO и подготовленные запросы (prepared statements).

Пример кода:

```php
public function getProducts(int $category_id, int $limit=12, int $page=0):
array
{
    $query = $this->db->prepare($this->queries['category_products']);
    $offset = $limit * ($page - 1);
    $query->bindParam(1, $category_id, PDO::PARAM_INT);
    $query->bindParam(2, $limit, PDO::PARAM_INT);
    $query->bindParam(3, $offset, PDO::PARAM_INT);
    return $this->executeQuery($query);
}

private function executeQuery(PDOStatement $query, $params=null): array
{
    try {
        $query->execute($params);
        return $query->fetchAll(PDO::FETCH_ASSOC);
    } catch (PDOException $e) {
        var_dump($e->getMessage());
        abort(500);
        die();
    }
}
```

XSS-атаки

Для защиты от данного рода уязвимостей используется метод htmlspecialchars.

Пример кода:

```
public function saveFeedback(array $params): void
{
    $mapped_params = array_map("htmlspecialchars", $params);
    $query = $this->db->prepare($this->queries['save_feedback']);
    try {
        $query->execute($mapped_params);
    } catch (PDOException $e) {
        var_dump($e->getMessage());
        abort(500);
        die();
    }
}
```