



PHP Scan
online code scanner

Как **защитить** веб-ресурс на PHP

от взлома, кражи пользовательской
информации и денег

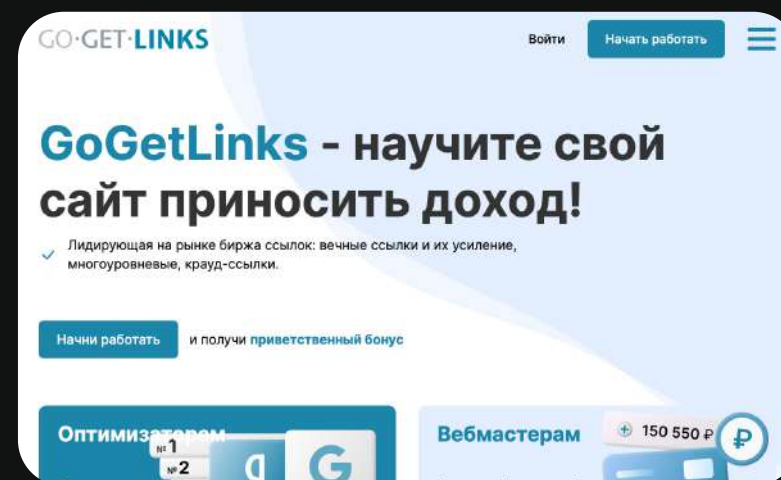
О нас: 15 лет экспертизы в PHP разработке

С **2009** года

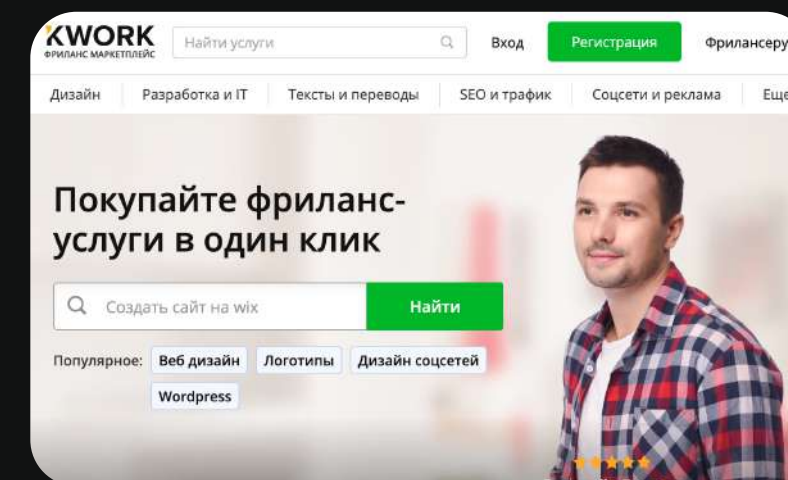
наша команда разрабатывает
крупные интернет-проекты на PHP

**Для нас безопасность
- не пустые слова!**

Наши проекты



Топ-3 крупнейших
бирж ссылок



Фриланс-площадка
№1 в рунете

Суммарно:

- > **10+ млн** зарегистрированных пользователей
- > **4,5 млн** посетителей в месяц
- > **1,5 млн** строк кода

Мы разработали решение по устранению уязвимостей в PHP коде

PHP Scan – не просто сканер уязвимостей, а инструмент по повышению безопасности проектов на PHP

1 Высокая точность сканирования без ложных срабатываний

1,5 года

заняла разработка сканера

1000

реальных проектов проверили с GitHub и GitLab

- ✓ Оттачивали сканер для безопасности своих инхауз проектов, работая на результат
- ✓ Сканер **обнаруживает уязвимости через логику** и нам не нужно скачивать базы известных уязвимостей

PHP Scan – инструмент по повышению безопасности

2 Качественные рекомендации по исправлению ошибок безопасности на основе нашей экспертизы

Мы – носители экспертизы
и глубоко разбираемся в PHP



Передаем свой **15 летний** опыт

по выстраиванию безопасности для крупных и популярных проектов



Любой программист,

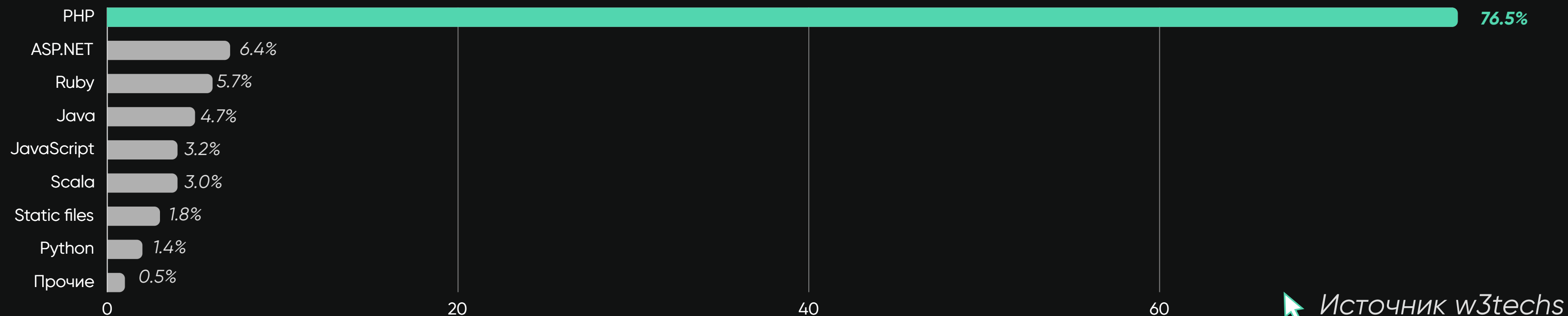
прочитав наши рекомендации, сможет исправить уязвимость

3 Возможность обратиться к нашим специалистам по безопасности за дополнительными пояснениями и рекомендациями

Это актуально и ценно,

когда на рынке не хватает грамотных AppSec специалистов
и они стоят очень дорого ~ 400 000 руб в мес

77% веб-приложений написаны на PHP



Если у вас приложение на таких CMS



значит, у вас
приложение на PHP

Уязвимости приводят к опасным рискам

Несанкционированный доступ

к информации клиентов, изменение
и потеря данных



Кража денег

с аккаунтов пользователей и
компании



Раскрытие персональных данных и серьезные штрафы

до
500 млн.
руб. от регулирующих
органов



*23 января 2024 года Госдума одобрила законопроект
об административной и уголовной ответственности за
нарушение защиты персональных данных (ФЗ №152)*

Полное или частичное прерывание работы сайта и бизнес-процессов

*Простой, потеря денег,
репутации и доверия клиентов*



Потеря управления над сайтом

и его полное уничтожение



Громкие взломы 2023 – 2024 годов

В сеть выложили 99 млн строк базы данных клиентов "Спортмастера"

Январь
2023

Февраль
2024

Роскомнадзор расследует инцидент с утечкой 510 млн записей о персональных данных россиян в 2024 г.

"Яндекс" подтвердил утечку исходного кода своих сервисов

Январь
2023

Утечки информации

В 2023 году число утечек данных из компании и госорганов в России возросло в разы*

Февраль
2023

"Магнит" подтвердил утечку персональных данных сотрудников магазинов "Дикси"

Утечка данных 97 млн пользователей сервиса электронных книг "ЛитРес"

Август
2023

Июнь
2023

"Ашан" подтвердил утечку данных покупателей, около 8 млн записей

Риск атак ежегодно **растет на 13%**

Заголовки новостей

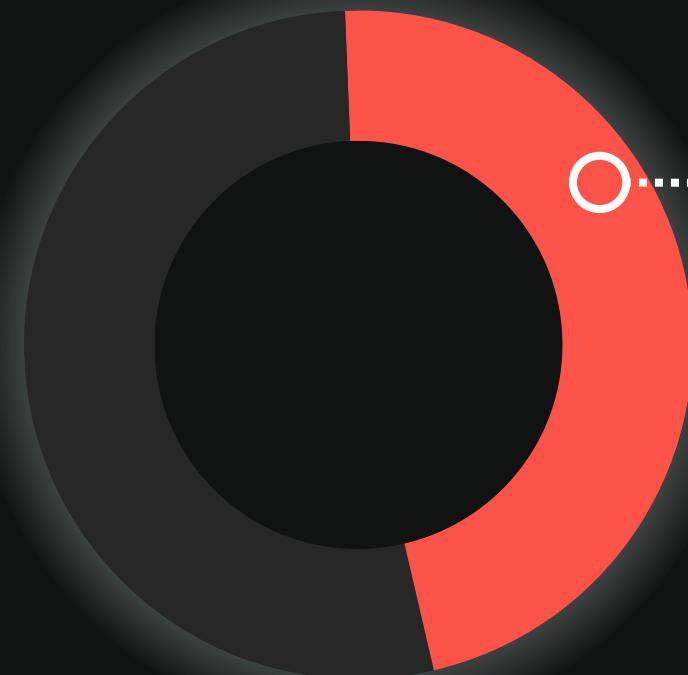
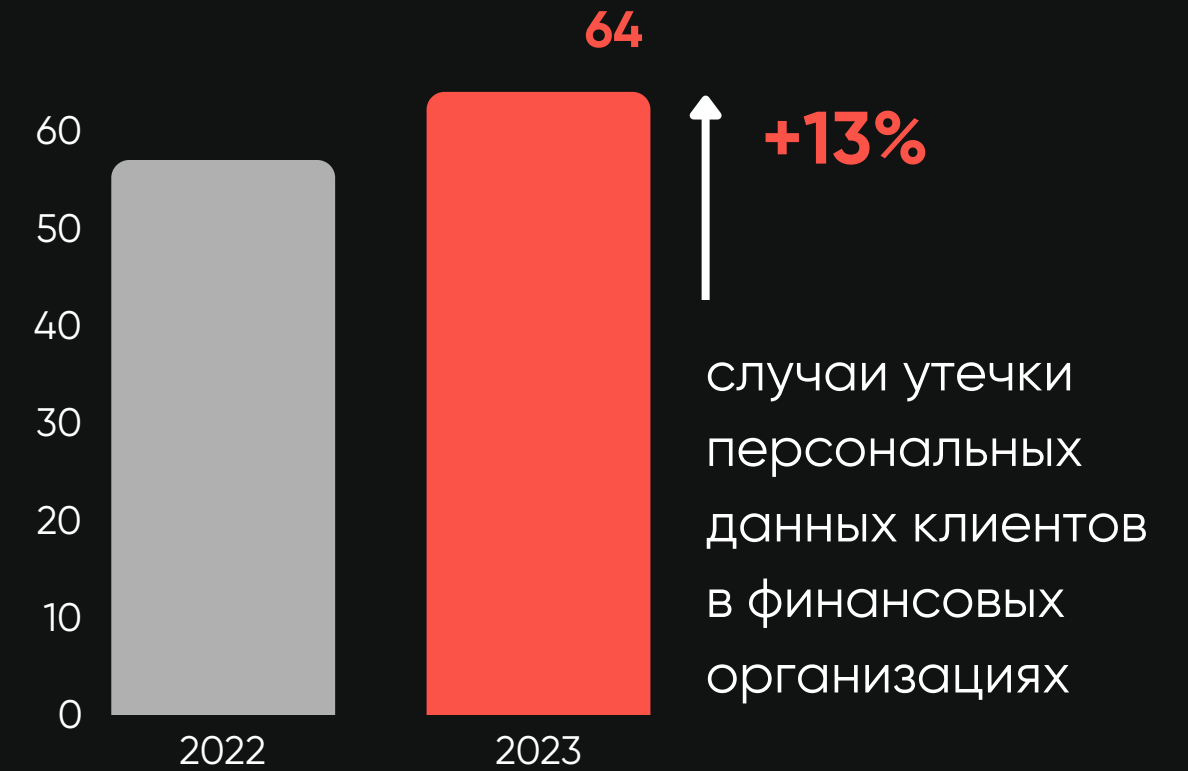
“В открытый доступ попали данные клиентов **Альфа-банка**”

“Роскомнадзор подтвердил утечку данных 1 млн клиентов **МТС-банка**”

“В сеть попали данные 47 млн пользователей «**СберСпасибо**»”

170,3 млн

записей персональных данных клиентов утекло в 2023 году из банков и финансовых компаний



47% утечек приходится на банки

Проблема также фиксируется в микрофинансовых организациях, платежных сервисах, на криптобиржах, традиционных биржах и др

Как обычно защищают приложения?

- ↓ Заказывают пентест
- ↓ Закрывают дыры с помощью внешнего контура защиты WAF (брандмауэр веб-приложений)
- ↓ Внедряют DAST

✓ Считается, что **WAF**
-это оперативное решение для защиты веб-приложений даже при наличии критичных уязвимостей

НО

WAF **НЕ способен защитить** веб-приложение от серьезных уязвимостей
т.к. описаны многочисленные **методы обхода WAF и реализации SQLi-атак и XSS**

🖱️ (Источник Positive Technologies)

🗑️ WAF не панацея, а временное решение

🗑️ WAF не помогает устранять уязвимость

🗑️ WAF лишь прикрывает вектор атаки

Если НЕ устранить уязвимость, будьте готовы к утечке конфиденциальных данных

Пострадавшие компании от SQLi-атак:



Tesla



Cisco



Fortnite
(онлайн игра с
350 млн игроков)



Freepik

Украдено

100 млн

данных платежных карт

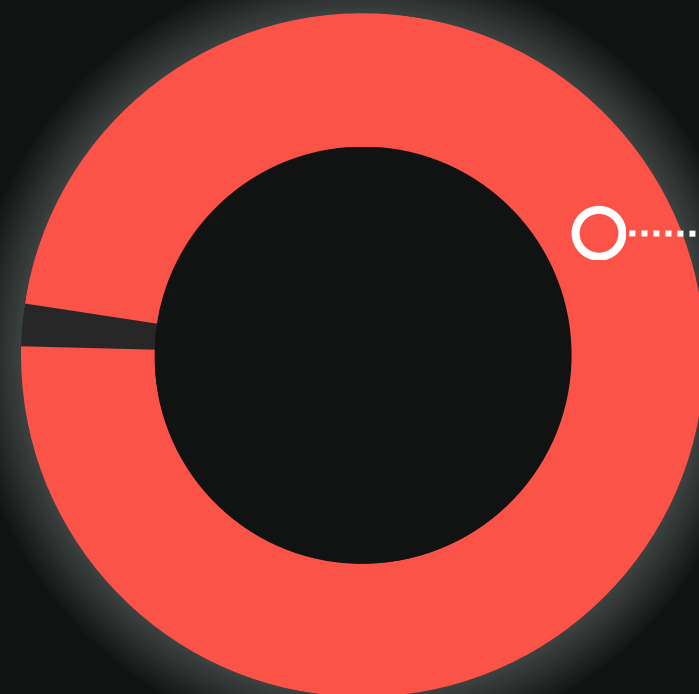
Выплачено

200\$ млн

компенсаций

Утечка данных, связанная с SQL-уязвимостью, обошлась компании **Heartland** (Американская платежная система) в \$200 млн штрафов и компенсаций клиентам, а также падением цены акций на 77%.

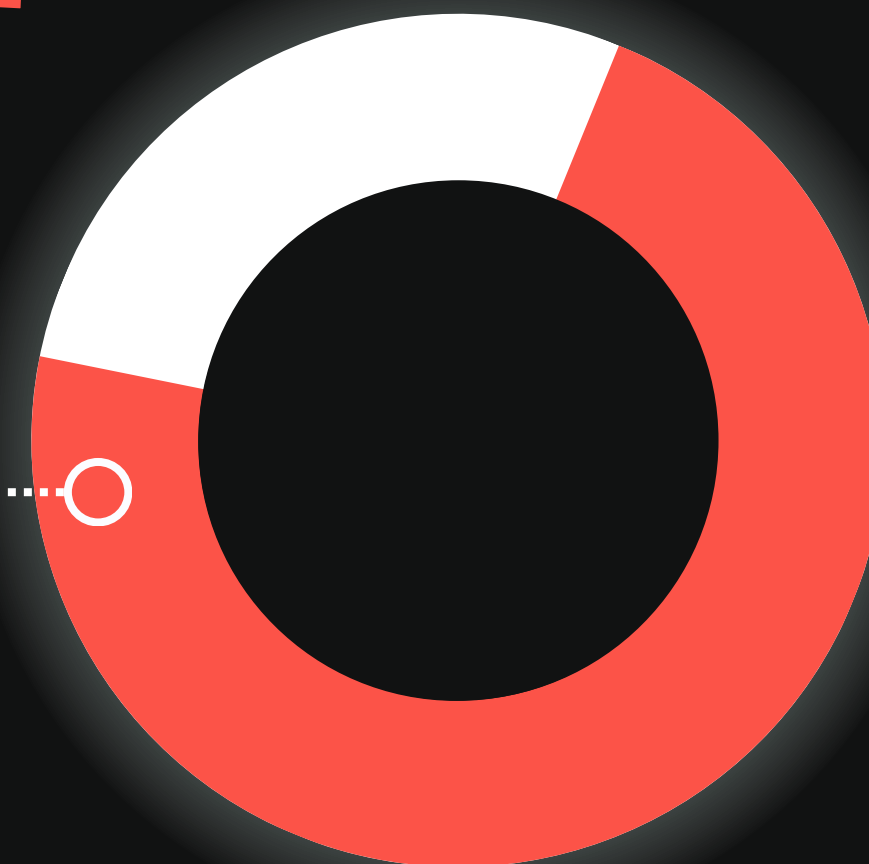
Чтобы устранять
уязвимость, **нужно**
проверять код



98% веб-приложений уязвимы

**по данным исследований
Positive Technologies в 2020-2021*

72% всех найденных
уязвимостей связаны
с ошибками в коде,
что подтверждает
необходимость
сканировать код



Какой сканер для проверки кода **лучший** в мире?

Мы проанализировали рынок сканеров уязвимостей.

Критерии выбора лучших решений для проверки PHP кода:



Мировые SAST РЕШЕНИЯ для проверки PHP кода

Название	Оценка компании	Трафик по SimilarWeb
Sonarqube от Sonarsource	\$4.7 млрд на 2022 год	1 М
Snyk Code	\$3.3 млрд на 2023 год	1.4 М
Sonatype	\$0.13 млрд на 2012 год	0.5 М
Solar appScreeener 	-	0,2 М
Semgrep Code	-	0.1 М
CloudDefense.AI's SAST	-	0.08 М
Aikido.dev	-	0.01 М
Application security от GitLab	-	-
PHP Scan 	new	new

**Для сравнения
взяты популярные в
мире анализаторы
статического кода*

Мировые SAST решения для проверки PHP кода

По ряду известных сканеров тесты **НЕ** проводились ввиду:

┌ Принадлежности к DAST
(Veracode, Rapid7, Acunetix, Fortify WebInspect, PT Application Inspector и другие)

┌ Отсутствия
 возможности протестировать

┌ Дорогостоящих проверок

SAST сканеры, не вошедшие в тестирование на качество проверки кода:

Название	Оценка компании	Трафик по SimilarWeb	Цена, в мес.	Возможность протестировать
HCL AppScan	\$4.5 млрд	185 К	Через запрос	Через запрос
Checkmarx	\$1.15 млрд	142 К	Через запрос	Через запрос и предпродажные скрипты
Mend SAST (от Mend.IO)	\$0.75 млрд	124 К	от 1 600 000 руб в мес	
PT Application Inspector 	\$0.7 млрд	244 К	420 000 руб в мес	Через опросники и длительные ожидания ответов
CAST AIP	\$0.05 млрд	108 К	от 9 000 000 руб в мес	

Проверка сканеров на качество сканирования кода

✓ Мы сформировали
225 ТЕСТОВ

из реальных фрагментов кода с GitLab,
GitHub и наших коммерческих проектов

✓ Учли

- каждый тип уязвимостей по стандарту CVSS с разными вызовами функций, получением данных
- разные версии php и разные конструкции, которые там используются

1

ЭТАП
Подготовка
тестов

В тестах содержатся как реальные уязвимости, так и направленные на ложноположительные срабатывания

Проверка сканеров на качество сканирования кода

2

ЭТАП

Проверка кода
всеми сканерами

3

ЭТАП

Расчет качества
сканирования

По каждому сканеру посчитали,

- сколько уязвимостей он нашел правильно (TP)
- сколько уязвимостей он не нашел (FN)
- в скольких случаях указал на уязвимость, хотя ее нет (FP)
- в скольких не нашел уязвимостей, что верно (TN)

Для каждого сканера
рассчитали **точность сканирования**
по следующей формуле:

True Positive (TP)	False Positive (FP)
False Negative (FN)	True Negative (TN)

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Пример результатов тестирования

* Тестовый код, а также подробные результаты сканирования по каждому сканеру могут быть высланы по запросу.

Сравнение php SAST

Файл Правка Вид Вставка Формат Данные Инструменты Расширения Справка



100% | р. % .0 .00 123 | По ум... | - 10 + | B I A

B55 | fx =(B54+C54)/(B54+C54+D54+E54)

	A	B	C	D	E	F	G	H	I	J
1	Группа тестов	True Posivite	True Negative	False Positive	False Negative	Что и где он нашел				
32	escaped_sql	1	9	0	10	src_interval_scope/wp-includes/taxonomy.php - в строках 5071				
33	extend_pdo	1	1	0	2	src_literal_empty_string/index.php - в строках 9, 18				
34	extract	0	1	0	2	src_multi_extends/index.php - в строках 14				
35	extract_unknown_taint	1	1	0	0	src_mysql_escape_string/index.php - в строках 22				
36	fallthrough_context	0	2	0	1	src_mysql_query/index.php - в строках 4				
37	fallthrough_is_numeric	1	1	0	0	src_pdo/run.php - в строках 13				
38	fallthrough_not_intval	1	0	2	0	src_php82/Input.php - в строках 32, 41, 49				
39	headers	1	0	0	0	src_php82/readonly.php - в строках 13				
40	instanse_of	2	0	0	0	src_property/T.php - в строках 14				
41	internal_safe_type	0	1	0	1	src_short_open_tag/index.php - в строках 5				
42	interval_scope	2	0	0	0	src_source_details/index.php - в строках 6, 13, 28, 35, 42, 51				
43	literal_empty_string	0	1	2	1	src_switch_const/index.php - в строках 18, 26				
44	multi_extends	1	0	0	0	src_test1/m_test_db.php - в строках 30, 31, 34				
45	mysql_escape_string	1	2	0	2	src_test2/m_test_db.php - в строках 13				
46	mysql_query	1	0	0	0	src_test2_1/m_test_db.php - в строках 30				
47	pdo	1	1	0	2	src_test3/z-ele-custom-skin.php - в строках 29				
48	pdo_1	0	1	0	3	src_test4/test_db.php - в строках 46				
49	pdo_2	0	1	0	3	src_unary_op/index.php - в строках 45, 46, 47, 48, 49				
50	php82	4	2	0	2	src_interval_scope/wp-includes/functions.php - в строках 4064				
51	preg_reddos	2	0	0	0	src_xss_printf/index.php - в строках 5				
52	property	1	0	0	0	src_unserialize/index.php - в строках 4				
53	session	0	0	0	1	src_preg_reddos/index.php - в строках 5, 9				
54	Summary	34	63	13	55					
55	Accuracy	58,79%								
56										

+ Summary PhpSecure SonarQube 4 Snyk Semgrep aikido CloudDefense/GitLab/SonaType

Результат сравнения сканеров

Название	Точность сканирования	Цена, в месяц <i>(для типового проекта с 1 млн строк и 25 разработчиками)</i>	Оплата из России	Интеграция с Git
CloudDefense.AI's SAST	7%	По запросу	✗	✓
Sonatype	7%	16 500 руб (\$165 за 25 разработчиков)	✗	✓
Application security от GitLab	7%	Бесплатно	✗	✓
Aikido.dev	41%	80 000 руб (тариф Standard на 30 разработчиков)	✗	✓
Semgrep Code	43%	100 000 руб (25 разработчиков по \$40 в месяц)	✗	✓
Solar appScreeener 	45%	192 000 руб (без интеграции с Git)	✓	✓
Snyk Code	53%	62 500 руб (25 разработчиков по \$25)	✗	✓
Sonarsource от Sonarqube	59%	35 000 руб	✗	✓
PHP Scan – NEW 	95%	20 000 руб * Бесплатный доступ, пока сканер находится в beta-версии	✓	✓

Как мы добились **высокого качества проверок PHP Scan?**

PHP Scan **смотрит логику** программы и **защищает** от потенциальных уязвимостей

Нас часто спрашивают, как обновляются базы уязвимостей в статическом анализаторе кода?

Важно понимать, что

Статический анализатор

– это не антивирус



здесь **не нужно** постоянно скачивать базы известных уязвимостей



статический анализатор смотрит логику и защищает от всех потенциальных уязвимостей

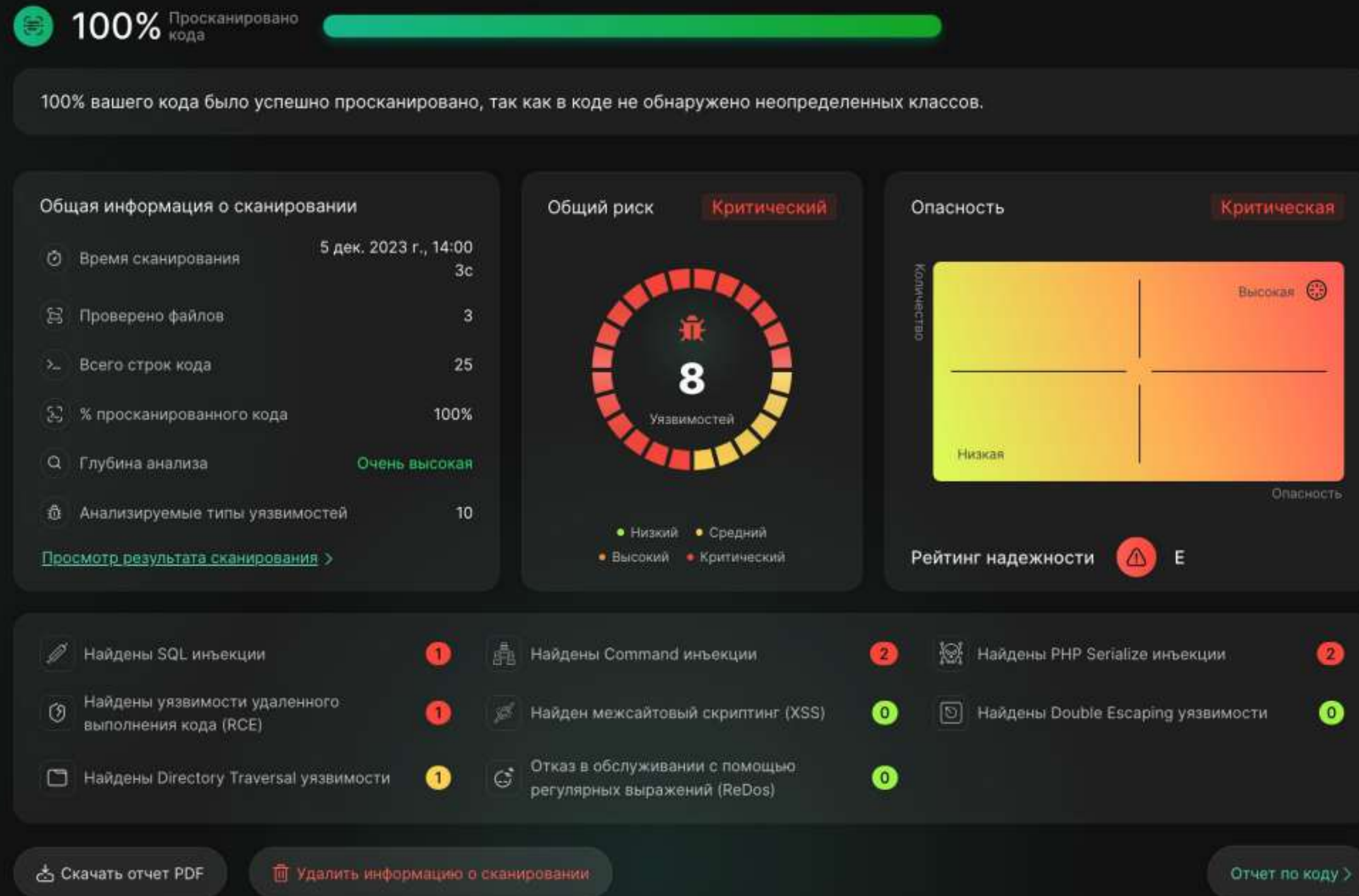
Мы защищаем от уязвимостей

не только от имеющихся, но и от тех которые могут появиться, потому что анализируем все обращения к базе данных (на примере SQLi)

Мы организовали обнаружение уязвимостей

через логику, потому что глубоко разбираемся в PHP.

Лучшее SAST решение для проверки PHP кода



PHP Scan обнаруживает наиболее распространенные и опасные типы уязвимостей для PHP-приложений:

- ✓ SQL инъекции
- ✓ Command инъекции (Shell)
- ✓ Cross-Site Scripting (XSS)
- ✓ PHP Serialize инъекции
- ✓ Удаленное выполнение кода (RCE)
- ✓ Directory Traversal
- ✓ Отказ в обслуживании с помощью регулярных выражений (ReDos)

Лучшее SAST решение для проверки PHP кода

PHP scan дает:

Детальный отчет о найденных уязвимостях кода

Пояснения, почему это уязвимость

Откуда идет уязвимость

The screenshot displays the PHP Scan interface with the following components:

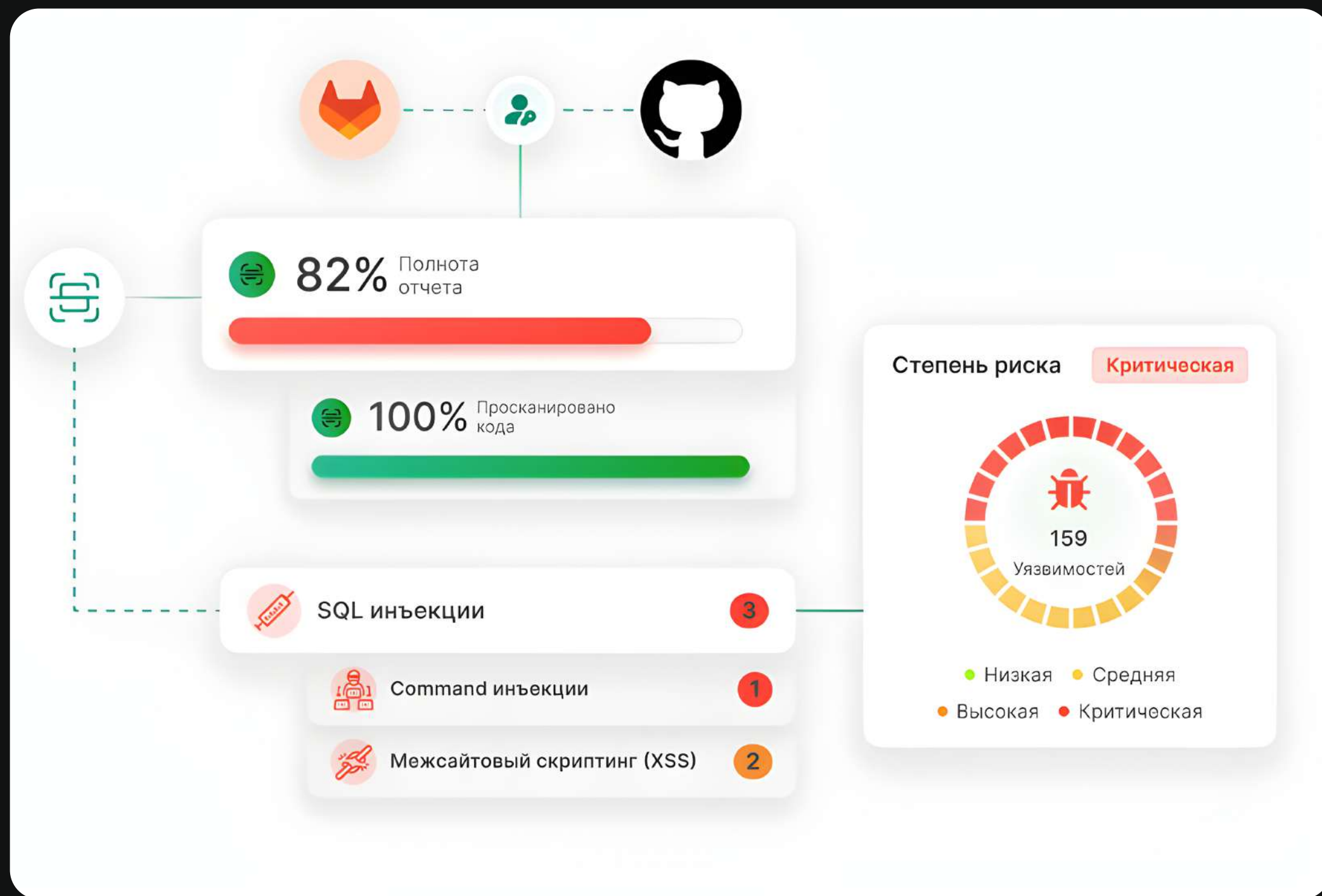
- Header:** "Данные об уязвимостях" (Vulnerability Data) with filters for "Группировать без условий" and "Сортировать сначала опасные".
- Summary:** "3 из 3 уязвимостей" (3 of 3 vulnerabilities).
- STATUS:** A list of status options: "Открыт" (3), "На исправлении" (0), "Исправлен" (0), "Проигнорирован" (0).
- УРОВЕНЬ РИСКА (Risk Level):** "Критично" (1), "Высокий риск" (1), "Средний риск" (1), "Низкий риск" (0).
- ТИПЫ УЯЗВИМОСТЕЙ (Vulnerability Types):** "SQLi" (0), "Command инъекция" (1), "PHP Serialize инъекция" (0), "RCE" (0), "XSS" (1), "Double Escaping" (1), "Directory Traversal" (0), "ReDoS" (0).
- Command инъекция (Command Injection):** File: "builds/test1570636/test-many-vulns/command_-_shell.php".
 - Code Snippet:** Line 3: `exec($_GET["cmd"]); // src/1.php:3 SecurityCheck-ShellInjection Calling method \exec(["var"]) in [no method] that outputs using tainted argument #1 ($_GET['cmd']).`
 - Description:** "Обнаружена командная инъекция. Измените этот код, чтобы он больше не передавал небезопасные данные, предоставленные пользователем." (Command injection detected. Change this code so it no longer passes unsafe data provided by the user.)
 - Details:** A JSON object describing the source, keys, file, and destination of the vulnerability.
 - Actions:** "Игнорировать", "Отметить как на исправлении", "Путь уязвимости".
- XSS:** File: "builds/test1570636/test-many-vulns/XSS.php".
 - Code Snippet:** Line 5: `printf("Hello, %s", $login);`
 - Actions:** "Открыт".

Автоматическое сканирование кода

- ✓ **Полная поддержка по внедрению сканирования кода в CI/CD Pipeline от наших специалистов**

интегрируйте сканер в ваш Git репозиторий

При каждом обновлении код будет автоматически сканироваться.



Как сканировать код с PHP Scan?



 www.phpscan.com

1

Вариант SaaS решение



PHP Scan гарантирует **полную конфиденциальность** вашего кода и отчетов об уязвимостях

- ✓ **Код безвозвратно удаляется с сервера**
 - Сразу после загрузки и сканирования
 - Чтобы повторить сканирование, нужно повторно загрузить свой код или указать путь к GIT-хранилищу.
 - ✓ **PHP Scan не использует и не передает загружаемый код кому бы то ни было**
 - ✓ **Сканер полностью зашифрован**
- Это обеспечивает максимальную безопасность данных**

Как сканировать код с PHP Scan?

2

**Вариант
Self-hosted решение**

**на серверах
клиентов**

**Будет реализовано
~ через 2 недели**

Мы также можем для вас:

✓ **Провести демо-созвон**

с презентацией
сканера в деле

✓ **Проконсультировать**

по найденным
уязвимостям и как их
исправить

✓ **Настроить сканирование**

фрагментов кода
проекта или всего
проекта целиком

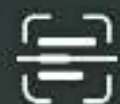
✓ **Помочь с интеграцией сканера**

в ваш GitLab или GitHub для автоматических проверок
кода и расширения CI/CD процесса

Доступное сканирование

2 месяца
Бесплатная тестовая лицензия

Попробуйте и убедитесь сами в качестве сканирования и рекомендациях по исправлению кода.



Введите название ваш...

Начни сканирование бесплатно!

Дальше стоимость сканера

20 000

руб в **месяц**

150 000

руб в **год**



Безлимитное сканирование кода



Нет переплаты

за дорогие, но неэффективные для PHP решения, которые стоят ~ 100 000 руб в месяц

Выгода использовать PHP Scan:

Снижение рисков потери денег и убытков от взлома



₽ 1 000 000 000

Максимальные убытки
от утечки



₽ 27 700 000

Средние убытки
от утечки



₽ 10 500 000

Средние ожидаемые
убытки от утечки



₽ -

Защищенный проект -
минимум рисков

Выгода использовать PHP Scan:

Снижение рисков потери денег и убытков от взлома



Защита от взлома,

утечки конфиденциальных данных и финансов, парализации бизнес-процессов или полного уничтожения проекта.



Сокращение рисков получить высокий штраф

от регулирующих органов за утечку персональных данных.

Выгода использовать PHP Scan: Снижение рисков потери денег и убытков от взлома



**Консультация по исправлению
найденных уязвимостей**

от специалистов по безопасности PHP Scan



Учет пожеланий по доработке сканера

исходя из ваших бизнес задач и процессов
разработки

Планы на будущее по PHP Scan

Мы работаем над постоянным усовершенствованием сканера, чтобы предоставлять **комплексное решение по безопасности**

30+

ЯЗЫКОВ
ПРОГРАММИРОВАНИЯ

**Проверка на полный
спектр угроз,**

в том числе ошибки
конфигурации, уязвимости
во вспомогательном ПО

**Эволюция сканера из SAST
в IAST решение, которое
будет анализировать:**

- потоки данных
- конфигурацию
- HTTP-запросы и ответы
- библиотеки, фреймворки и другие компоненты
- информацию о внутреннем подключении

Партнерство с вендорами и интеграторами

Вы можете

расширить спектр своих услуг за счет интеграции статического анализатора кода.

Это даст дополнительный доход и лояльность клиентов за счет новой ценной услуги.

Мало, кто это предлагает, особенно с индивидуальной поддержкой и разборами инцидентов от специалистов по безопасности.



 https://t.me/Julia_guidera



Юлия Котова

Руководитель проекта

Мы открыты для партнерства

Спасибо за внимание!



PHP Scan
online code scanner

www.PHPScan.com

Есть вопросы? **Пишите!**



CEO PHP Scan
Юлия Котова

