**Универсальные сканеры безопасности веб-сайтов**

[**1. Acunetix**](https://www.acunetix.com/vulnerability-scanner/website-vulnerability-scanner-online/)

Классический коммерческий сканер. Проверяет сайты на множество уязвимостей. Требует регистрацию на корпоративный почтовый ящик. Есть бесплатное использование на протяжении 14 дней. Сервис дает полезные результаты.

[**2. Detectify**](https://detectify.com/)

Коммерческий сканер безопасности сайтов, который позволяет проводить несколько десятков автоматических тестов безопасности, включая тесты OWASP Top 10, тесты на наличие вредоносного программного обеспечения и многие другие. Сервис требует регистрацию, работает бесплатно только 14 дней. Сканирование идет несколько часов и дает приличное количество результатов.

[**3. H-X Scanner**](https://h-xtech.com/ru/scan)

Бесплатный онлайн-сканер. Имеет два режима: быстрый и нормальный. Не требует регистрации: нужно ввести адрес вашего сайта и адрес электронной почты для получения отчета. В быстром режим весь процесс сканирования занимает пять минут. Процесс нормального сканирования занимает от нескольких минут до нескольких часов, в зависимости от сложности и объема.

[**4. ImmuniWeb**](https://www.immuniweb.com/websec/)

Сервис бесплатен и имеет простой, удобный и продуманный функциональный интерфейс. Сканер проверяет безопасность сервера вашего сайта, его соответствие требованиям стандартов PCI DSS и GDPR, заголовки HTTP, включая CSP, выполняет специфические тесты CMS для сайтов на базе WordPress и Drupal, проверяет уязвимости библиотек интерфейсов и многое другое. Работает не очень быстро, но предоставляет удобные и наглядные результаты.

[**5. Intruder**](https://www.intruder.io/?utm_source=referral&utm_campaign=geekflare_online_scan_website_security_vulnerabilities)

Современный коммерческий сканер широкого спектра уязвимостей. Сервис имеет расширенные возможности вроде анализа безопасности облачных систем и API. Удобен в использовании. Требует регистрацию. Бесплатен на протяжении 30 дней.

[**6. Netsparker Cloud**](https://www.netsparker.com/online-web-application-security-scanner/)

Один из классических коммерческих сканеров. Конкурент Acunetix. Пробная бесплатная версия действует также 14 дней. Требует корпоративную регистрацию, предоставляет относительно много результатов.

[**7. Norton Safe Web**](https://safeweb.norton.com/)

Сканер бесплатный и легко запускается, но не дает результатов, если только ваш сайт уже не находится в базе данных сервиса.

[**8. Observatory**](https://observatory.mozilla.org/)

Бесплатный сервис от знаменитого проекта Mozilla. Сканер помог владельцам нескольким десяткам миллионов веб-сайтов. Сервис простой в использовании, быстрый и наглядный. Он проверяет безопасность заголовков HTTP, выполняет тесты SSL, TLS, предварительной загрузки HSTS и т.д.

[**9. Pentest-Tools**](https://pentest-tools.com/website-vulnerability-scanning/website-scanner)

Быстрый и простой в использовании сканер, имеющий бесплатную и платную части. Бесплатное сканирование можно запустить только два раза. Оно не требует регистрации, но предоставляет ограниченные результаты.

[**10. Probely**](https://probely.com/)

Платный сканер уязвимостей имеет качественный пользовательский интерфейс и возможность пробного бесплатного использования в течение 14 дней. Регистрация и использование несложные. Probely удобен для разработчиков сайтов и веб-приложений. Он содержит не только функции поиска уязвимостей, но и полного цикла управления ими, включая их устранение. Сервис работает достаточно быстро, в бесплатном режиме выдает ограниченное количество результатов.

[**11. Quttera**](https://quttera.com/)

Бесплатный инструмент, в некоторой мере аналогичен Sucuri, описанному ниже, но дает немного больше результатов. Работает тоже немного дольше, хотя в целом довольно быстро — несколько десятков секунд. Сканер прост в использовании и позволяет проверить сайт на некоторый ограниченный перечень уязвимостей, наличие вредоносных и подозрительных файлов, а также анализирует присутствие сайта в списках безопасного просмотра и вредоносных программ.

[**12. Sucuri SiteCheck**](https://sitecheck.sucuri.net/)

Бесплатный сканер Sucuri оставляет неплохое впечатление. SiteCheck прост в использовании. Работает со всеми типами сайтов, а не только WordPress. Сервис имеет довольно ограниченный функционал — проверяет присутствие сайта в списках безопасного просмотра (Google, «Яндекс» и т.д.) и в черных списках, проверяет наличие файервола, мониторинга, некоторого вредоносного ПО, а также некоторых протоколов и заголовков.

[**13. SiteGuarding**](https://www.siteguarding.com/en)

Сервис сканирует сайты на наличие вредоносных программ, проверяет черные списки, спам и т.д. Сканер декларирует, что распознает WordPress, Joomla, Drupal, Magento, osCommerce, Bulletin и другие платформы.

[**14. Tinfoil Security**](https://www.tinfoilsecurity.com/solutions/web-scanner)

Инструмент платный, с возможностью бесплатного демо. Настройка Tinfoil Security умеренно сложная. Отдельные тесты проводятся, даже если сайт защищен паролем, или для входа требуется регистрация. Есть функционал мониторинга.

[**15. UpGuard Scan**](https://www.upguard.com/)

Этот платный инструмент выполняет оценку рисков. Он использует информацию о различных параметрах сайта. Пробная бесплатная версия действительна 7 дней.

[**16. VirusTotal**](https://www.virustotal.com/)

Знаменитый агрегатор антивирусов, который приобрела компания Google. Имеет также функцию агрегации черных списков сайтов. Работает бесплатно, максимально просто и мгновенно выдает результаты.

**Сканеры безопасности сайтов на базе WordPress**

[**17. IsItWP Security Scanner**](https://www.isitwp.com/wordpress-website-security-scanner/)

Бесплатный, простой в использовании, не требующий регистрации сканер на базе движка Sucuri, с двумя недостатками: 1) скорость работы, 2) функционал ограничен только некоторыми проверками (в основном, на известное вредоносное ПО).

[**18. Web Inspector**](https://www.webinspector.com/)

Онлайн-сканер для проверки безопасности сайтов на базе WordPress. Сервис сканирует сайт с помощью Google Safe Browsing и движка Comodo. Сканер проверяет, есть ли вредоносный код, бэкдоры, вирусы, подозрительные скрипты и файлы.

[**19. Wprecon**](https://wprecon.com/)

Сканер бесплатен, прост в использовании и достаточно быстр. Среди систем своего класса имеет наиболее подробные и удобные отчёты, а также ссылки на дополнительный функционал. Инструмент проверяет версию WordPress, плагины, темы, идентификацию пользователей, индексирование каталогов, iframes, ссылки, JavaScripts и так далее. Результаты достаточно полные.

[**20. WPsec**](https://wpsec.com/)

Сканер сайтов на WordPress с ограниченной бесплатной версией. WPsec использует распространенный бесплатный движок WPscan — сканер уязвимостей, работающий в командной строке. Он предоставляет информацию об устаревших версиях WordPress, его компонентов и других недостатках безопасности.

**Бонус**

[**21. Google Safe Browsing**](https://transparencyreport.google.com/safe-browsing/search)

Это не сканер, а просто интерфейс к «черному списку» Google, то есть к базе данных, содержащей списки вредоносных сайтов. Многие сканеры, упомянутые в этом обзоре, используют Google Safe Browsing для своих результатов. Сервис интегрирован с Google Search Console. Если вдруг ваш сайт окажется в «черном списке», вы получите подробные инструкции о том, как удалить его оттуда. Сервис бесплатен, не требует регистрации, прост в использовании и быстр, но не проверяет сайты на уязвимости.