УДК 004.77

Селенков Александр Сергеевич
студент 3 курса магистратуры,
информационный факультет
Донской государственный технический университет,
Россия, г. Ростов-на-Дону
e-mail: selenkov.a@mail.ru

ЯВЛЯЕТСЯ ЛИ WORDPRESS БЕЗОПАСНЫМ?

Аннотация*. Данная статья, рассматривает систему управления контентом «WordPress» на вопрос ее безопасности. Проводя исследование, были проверены более 40 тыс. сайтов. Результат проверки, подтвердил, что более 70% сайтов уязвимы к атакам.*

Ключевые слова. WordPress, безопасность, сайты, взлом.

Selenkov Alexander Sergeevich
3rd year master student,
faculty of information
Don state technical University,
Russia, Rostov-on-don

IS WORDPRESS SECURE?

Annotation. This article examines the content management system "WordPress" on the issue of its security. During the research, more than 40 thousand sites were checked. The result of the check confirmed that more than 70% of sites are vulnerable to attacks.

Keyword. WordPress, security, sites, hacking.

Является ли wordpress Небезопасным?

Wordpress занимает самую большую долю рынка среди систем управления контентом и 30% рынка среди самых популярных 10 миллионов сайтов в интернете. Такой успех делает его большой мишенью для хакеров. Wordpress не менее безопасен, чем другие системы управления контентом — он просто более успешен.

Уязвимости в ядре wordpress ответственны менее чем за 10% всех взломов wordpress. Большинство из них-от устаревших установок wordpress. Количество взломов, которые происходят на реальных дырах безопасности в современных

версиях (также известных как эксплойты нулевого дня) в ядре wordpress, составляет крошечный процент всех взломов.

Остальные зараженные сайты были вызваны плагинами, темами, хостингом и пользователями. И вы, как разработчик сайта wordpress, имеете контроль над всем этим.

Кто чаще всего нападает на сайты?

В редких исключениях, бывают нападения на сайты, с личными намерениями нанести вред своему конкуренту, врагу или просто поэкспериментировать. В большинстве случаев, нападение осуществляют боты. Боты - это компьютерные программы, которые постоянно ищут сайты для взлома. Им все равно, кто вы, они просто ищут слабое место в вашей защите. Ботнет объединяет вычислительные мощности многих ботов для решения более крупных задач.

Для чего хакеры взламывают сайты?

Хакеры могут использовать уязвимости в вашем сайте для использования вычислительной мощности в своих целях, вымогательства и других целей. Основные причины для взлома сайта это:

- Рассылка спама
- Атака на другие сайты
- Кража ресурсов
- Продвижение других сайтов
- Кража данных

Почему Безопасность Имеет Значение?

Помимо того, что вы не даете преступникам удовлетворения, существует множество причин, по которым ваш сайт должен быть защищен по умолчанию. Очистив и разобравшись с большим количеством взломов wordpress можно с уверенностью сказать, что это всегда происходит неожиданно и в неудобное время. Уборка может занять не только продолжительное время, но и отнять много финансов.

Чтобы снова запустить взломанный сайт wordpress, вам нужно будет удалить и заменить каждый бит стороннего кода (включая ядро wordpress); прочесать свой собственный код строка за строкой и все другие папки на сервере, чтобы убедиться, что они все еще чисты; проверить, получили ли несанкционированные пользователи доступ; и заменить все пароли в wordpress, на вашем сервере и в вашей базе данных.

Множество сервисов могут очистить для Вас сайт wordpress, но профилактика в долгосрочной перспективе намного лучше.

После взлома, доверие к вашему сайту может упасть. Хаки перемещают вас ниже в рейтинге поиска, что приводит к меньшему количеству посетителей и меньшим конверсиям.

Больше, чем финансовые затраты, получение взлома вредит вашей репутации. Посетители приходят на ваш сайт, потому что они вам доверяют. Получение взлома наносит ущерб вашей репутации, и это занимает много времени, чтобы исправить.

Необходимые действия для обеспечения безопасности.

Триада ЦРУ - это базовая структура для каждого проекта цифровой безопасности. Он означает конфиденциальность, целостность и доступность. ЦРУ-это свод правил, который ограничивает доступ к информации нужных сторон, гарантирует достоверность и точность информации и гарантирует надежный доступ к этой информации.

Для WordPress фреймворк ЦРУ сводится к следующему.

- Конфиденциальность
- Целостность
- Доступность

Конфиденциальность

Убедитесь, что вошедшим в систему пользователям назначены правильные роли и что их возможности постоянно контролируются. Только дайте пользователям минимальный доступ, который им нужен, и убедитесь, что информация администратора не просочится не к той стороне. Вы можете сделать

это, укрепив админ-зону WordPress и будучи осторожными с именами пользователей и учетными данными.

Целостность

Покажите точную информацию на вашем веб-сайте и убедитесь, что взаимодействие пользователей на вашем веб-сайте происходит правильно.

Принимая запросы как на переднем, так и на заднем конце, всегда проверяйте, соответствует ли намерение фактическому действию. При публикации данных всегда фильтруйте данные в коде на наличие вредоносного контента с помощью дезинфекции и экранирования. Убедитесь, что спам удаляется с помощью службы защиты от спама, такой как Akismet.

Доступность

Убедитесь, что ваши WordPress, плагины и темы актуальны и размещены на надежном (предпочтительно управляемом) Хосте WordPress. Ежедневные автоматические резервные копии также помогают гарантировать, что ваш сайт остается доступным для общественности.

Все три элемента опираются друг на друга для поддержки. Целостность кода не будет работать сама по себе, если конфиденциальный пароль пользователя легко украсть или угадать. Все аспекты важны для надежной и безопасной платформы.

Охрана - это очень тяжелая работа. Помимо работы, которую можно выполнить в коде, в этой структуре есть огромный человеческий элемент. Безопасность-это постоянный процесс, он не может быть решен одним плагином.

Список литературы:

1. Безопасность WordPress [Электронный ресурс] // Режим доступа: URL: https://wp-kama.ru/question/bezopasnost-wordpress (дата обращения: 10.10.2020 г.).

2. Разрушаем миф: безопасно ли использовать WordPress для своего сайта. [Электронный ресурс] // Режим доступа: URL: https://www.anti-

malware.ru/analytics/Threats_Analysis/wp-security-myth (дата обращения: 10.10.2020 г.).

3. Безопасность Вордпресс. Полное руководство [Электронный ресурс] // Режим доступа: URL: https://techbear.ru/rukovodstvo-po-bezopasnosti-wordpress/. (дата обращения: 10.10.2020 г.).

4. Безопасность WordPress сайта под угрозой [Электронный ресурс] // Режим доступа: URL: https://seojus.ru/wordpress/bezopasnost-wordpress-sajta-pod-ugrozoj. (дата обращения: 10.10.2020 г.).