Таким образом, пользователь получает возможность вносить изменения в системные файлы, запускаемые им от имени суперпользователя (обладателя root прав). Например, становится возможным заменить suid-файл ping на системный терминал, который запустится от имени суперпользователя. Несмотря на то, что ошибка повышения привилегий реализуется исключительно среди локальных пользователей. Злоумышленники, не имеющие доступа к локальной сети, могут использовать уязвимость в сочетании с другими эксплойтами, которые предоставляют возможность удаленного управления и выполнение непривилегированного кода.

Использование такого сочетания инструментов не оставляет цифровых следов в системных журналах и приводит к полному взлому удаленной системы.

Список використаних джерел:

1. Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (SUID Method). URL: https://www.exploit-db.com/exploits/40616/ (дата звернення: 23.10.2017).

Одержано 30.10.2017

УДК 004.492.2

Ігор Володимирович КОБЗЕВ,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій і систем управління Харківського регіонального інституту державного управління Національної академії державного управління при Президентові України

Вікторія Анатоліївна ЛУК'ЯНОВА,
кандидат педагогічних наук, завідувач кафедри природознавчих наук Харківського національного університету радіоелектроніки

МЕТОДИ ЗАХИСТУ САЙТУ НА CMS WORDPRESS

Сфера інформаційної безпеки – актуальне питання сучасності. Захист сайтів від «хакерів» стає глобальною проблемою, над вирішенням якої працюють фахівці всього світу. Бізнес, побудований в агресивному середовищі Інтернет, уразливий і схильний до нападів з боку конкурентів і недоброзичливців. Єдиного інструменту для усунення усіх загроз несанкціонованого доступу до сайтів просто не існує [1].

WordPress є популярною безкоштовною системою управління контентом для сайтів. Відкрита форма WordPress використовується вже на 28,7 % світових сайтів. При цьому на ринку систем управління контентом (CMS) WordPress є

безперечним лідером за даними W3Techs web technologies з рейтингом 59,5 % [2]. На даний момент актуальною версією CMS WordPress є версія 4.8.2. Зокрема на WordPress працюють сайти освітніх установ та навчальних закладів, таких як Харківській національний університет радіоелектроніки (http://nure.ua/), Харківській політехнічний інститут (http://www.kpi.kharkov.ua/), Державний університет телекомунікацій (http://www.dut.edu.ua/), Академія Державної пенітенціарної служби (http://academy.kvs.gov.ua/), Міжнародний університет фінансів (http://iuf.edu.ua/) тощо.

Системи управління контентом (CMS), як і багато інших видів програмного забезпечення, досить уразливі. При цьому, чим поширенішою є система і чим частіше вона застосовується на популярних сайтах, тим більше грошей і зусиль зловмисники інвестують в пошук її проблемних місць. Крім того, більшість сучасних CMS складаються з безлічі модулів, і більшість уразливих місць пов'язані з плагінами, які зазвичай написані та протестовані на безпеку гірше, ніж основний код системи.

Основним недоліком WordPress, як і будь-якої іншої відкритої безкоштовної платформи для блогів, є її доступність для зловмисників.

Розглянемо декілька простих засобів захисту сайтів, які побудовано на CMS WordPress. Необхідно видалити користувача з логіном Admin. Зловмисникам набагато легше отримати доступ до вашого сайту за допомогою брут-форс атаки, особливо, якщо логін вже відомий. Найлегше зламати сайти, якщо використовується стандартний логін «admin» для адміністрування сайту.

Приховуємо версію Wordpress. Система автоматично вставляє номер поточної версії CMS в код кожної сторінки. Необхідно прибрати додавання в початковий код версії CMS WordPress. У файлі functions.php необхідно додати наступний код remove_action ('wp_head', 'wp_generator'). Також бажано видалити файл readme.html в кореневій теці сайту або можна використати плагін Remove WP version and shortlink.

Використовуємо файл .htaccess для захисту файлу wp-config (файл конфігурації сайту). .htaccess – це головний конфігураційний файл веб-сервера.

wp-config.php містить абсолютно усі дані, які потрібні для підключення до сервера MySQL, а також до бази даних. Необхідно знайти або створити файл .htaccess в корені сайту, та додати наступні рядки:

order allow, deny
deny from all

Необхідно обмежити кількість спроб доступу. Найчастіше зловмисники роблять величезну кількість спроб входу на сайт, підбираючи пароль. Можна налаштувати систему так, щоб IP-адреса була заблокована на декілька годин після певної кількості невдалих спроб входу. Для цього можна використати додаткові плагіни, наприклад, Login LockDown або Limit Login Attempts. У налаштуваннях цих плагінів, можна самостійно встановити кількість спроб входу і час блокування.

Додатково існує можливість прибрати відображення повідомлення про те, що введений логін і пароль невірні, адже це інформація також може допомогти зловмисникові.

Декілька складнішими є наступні засоби захисту:

– зміна префіксу таблиць баз даних за допомогою SQL-запиту PhpMyAdmin;

– використання SSL-сертифікату. Для передачі захищеної інформації і конфіденційності обміну даними рекомендується використовувати SSL-протокол. Необхідно придбати SSL-сертифікат і встановити його для доменного імені;

– використання двохфакторної автентифікації облікових записів. Після того, як ви вводите пароль на сайті, вам надсилається запит на новий одноразовий пароль, який ви отримуєте на контактний номер телефону або електронну пошту. Найпопулярніші плагіни двохфакторної верифікації WordPress – це Google Authenticator і Clef Two – Factor Authentication.

Отже можна зробити висновок, що забезпечення захисту сайту – це комплексне завдання, яке потребую чимало зусиль, і в умовах сьогодення є важливим та актуальним.

Список використаних джерел:

1. Кобзев И. В., Петров К. Е., Калякин С. В. Обеспечение безопасности сайта, построенного на системе управления контентом WordPress. *Системи обробки інформації.* 2012. Вип. 4(2). С. 37-41.
2. Usage Statistics and Market Share of Content Management Systems for Websites, October 2017. *W3Techs web technologies surveys.* URL: https://w3techs.com/technologies/overview/content_management/all (дата звернення: 10.10.2017).

Одержано 17.10.2017