Тези доповідей 52-ої наукової конференції молодих дослідників ОНПУ-магістрантів «Сучасні інформаційні технології та телекомунікаційні мережі» //Одеса: ОНПУ, 2017, вип. 52

ЗАСОБИ ПРОТИДІЇ ВРАЗЛИВОСТЯМ ПОПУЛЯРНИХ ДОПОВНЕНЬ ДЛЯ ІНТЕРНЕТ-ПРОЕКТІВ НА ПЛАТФОРМІ ″WORDPRESS″

Гулаткан С.С.

Науковий керівник – доц. каф. «Інформаційної безпеки», канд. техн. наук Задерейко О.В.

У теперішній час розробка інтернет-проектів будь-якого напрямку стала ще доступніша для кожного з нас, ніж раніше. Хтось має за мету ділитися з оточуючими своїми думками чи порадами, створюючи блог, інші прагнуть активно заробляти на своєму ресурсі різноманітними шляхами. В нашій статті звернемо увагу на той відсоток людей, які створюють сайти самостійно, без допомоги професіоналів та наслідки цього рішення. Їх дуже багато, тому приклад – велика кількість конструкторів інтернет-проектів та їх користувачів, наявність в інтернеті мануалів по створенню інтернет-проектів від ″А″ до ″Я″. Найбільш зручною та водночас ефективною платформою для створення інтернет-проектів загальної спрямованості прийнято вважати саме ″Wordpress″, у листопаді 2015 року за даними W3Techs (організація, яка займається аналізом технологій, що використовуються в інтернеті) 25% від усіх інтернет-проектів по світу працюють на цій платформі.

Створимо модель поведінки людини, яка вирішила створити інтернет-сайт для своїх потреб самостійно та не має в цьому необхідного досвіду: все починається з пошуку інформації в інтернеті, далі ця інформація відфільтровується та йдуть перші спроби того чи іншого прийому. В більшості випадків сайт буквально складають з частин функціонального та візуального оформлення, тобто використовують готові доповнення для платформи. Меншого ризику набувають новоспечені розробники, які встановлюють доповнення для свого сайту з офіціального сховища ″wordpress.org″, де шаблони та плагіни проходять модерацію і не містять явного натяку на вразливості. Якщо шукати шаблони на будь-яких інших сайтах, то у стовідсотковому порядку Ви отримаєте зовнішні посилання на рекламні сайти, як мінімум, а як максимум – серйозну вразливість, за допомогою якої сайт взагалі можна буде видалити, інше діло, що більшість звичайних інтернет-проектів нікому не потрібні. Це стосується не тільки шаблонів чи плагінів для нашої платформи, це стосується навіть для інтернет-проектів без платформи. Як підсумок, можна стверджувати, що звичайна людина

скоріше витратить свій час даремно, прагнучи з'явитися на теренах першої сторінки пошукової системи, або взагалі створить сайт, який зможе зламати кожен третій.

Повернемось до популярних доповнень, якими користуються майже усі, та їх вразливостей. Команда інтернет-сервісу по забезпеченню безпеки інтернет-проектів ″Sucuri″ проаналізувала ряд популярних плагінів в сховищі ″wordpress.org″ на використання функцій add_query_arg () і remove_query_arg (). Більшість виявилися незахищеними, серед них виділимо:

- Jetpack (3+ мільйонів діючих встановлень з директорії платформи; плагін, який додає загальної зручності у користуванні сайтом та пропонує відстеження статистики у адмін-панелі);
- All In one SEO pack (3+ мільйонів діючих встановлень з директорії платформи; плагін, який допомагає правильно настроїти внутрішню оптимізацію сайту);
- Google Analytics by Yoast (1+ мільйонів діючих встановлень з директорії платформи; плагін, який додає можливості інтегрувати сайт власника з сервісом відстежування відвідувачів Google Analytics);
- NextGEN Gallery (1+ мільйонів діючих встановлень з директорії платформи; плагін, який реалізує галерею з фото чи зображень в декількох видах).

Слідує відмітити, що сумарна кількість завантажувань кожного з перелічених плагінів перевищує 20 мільйонів.

Знайдені взразливості в усіх чотирьох плагінах треба віднести до розряду XSS (англ. *Cross Site Scripting* — міжсайтовий скриптінг″) — тип вразливості інтерактивних інформаційних систем у веб-середовищі. XSS виникає, коли на сторінки, які були згенеровані сервером, з якоїсь причини потрапляють користувацькі скрипти. Специфіка подібних атак полягає в тому, що замість безпосередньої атаки сервера зловмисники використовують вразливий сервер для атаки на користувача.

Ці плагіни використовують функції add_query_arg () і remove_query_arg () для того, щоб екранувати результат, але проблема у тому, що при відсутності аргументу $query ці функції використовують поточну адресу сайту, який знаходиться в глобальному масиві $ _SERVER ['REQUEST_URI']. При цьому,

знайдена адреса може використовуватися як є і може містити будь-яке введене значення (рис. 1).

```
$link = add_query_arg( 'foo', 'bar' );
printf( '<a href="%s">link</a>', $link );
```

Рис.1. Функція, яка виводить посилання.

На перший погляд може здатися, що ця функція додає аргумент до даного посилання і все правильно, але результат функції залежить від даної адреси та зловмисник може додати у кінці посилання ″?"><script>alert()</script>″ (рис. 2), тим самим виконати будь-який javascript код.

Рис.2. Виконання довільного javascript коду.

Для того, щоб це виправити, треба використовувати функції екранування esc_url() та esc_url_raw(), наприклад, після використання вразливих функцій(рис. 3).

```
$link = add_query_arg( 'foo', 'bar' ); // Небезпечно!
$link = esc_url( $link ); // Тепер нічого боятися.
printf( '<a href="%s">link</a>', $link );
```

Рис.3. Приклад правильного використання вразливих функцій.

У разі роботи з редиректами або ″HTTP API″ у ″Wordpress″, замість esc_url () слід використовувати функцію esc_url_raw (), яка екранує адресу, але не готує її для виведення на екран.

Говорячи про плагін NextGEN Gallery, треба згадати, що крім XSS вразливості були ще знайдені вразливості щодо SQL-запитів. Плагін некоректно обробляє user input таким чином, ніби user input помістили всередину прямого SQL-запита. Використовуючи це, можно змінити параметри запиту так, що NextGEN Gallery виконає потрібні нам дії. Розробники даного плагіна відразу після проведеної роботи спеціалістами Sucuri видали нову версію свого продукту,

де вказали, що ″поправили теги″, але ретельний аналіз показує що саме було виправлено.

Як підійти до проблеми захисту свого майбутнього чи існуючого інтернет-ресурсу? По-перше, краще довірити це спеціалістам з інформаційної безпеки. По-друге, слідувати порадам по уникненню виникнення потенціальних загроз.

Якщо ж власник інтернет-ресурсу вирішив самостійно займатися цим питанням, то йому слід звернути увагу на такі поради:

- Завантажувати шаблони, плагіни тільки з офіційного сховища ″Wordpress.org″;

- Не звертати увагу на платні шаблони, плагіни, які викладені у загальному доступі, так як там 100% є загрози;

- Видаляти доповнення, які не використовуються;

- Намагатися використовувати якомога менше доповнень;

- Завжди слідкувати за тим, щоб використовалися тільки останні версії доповнень та самої платформи ″Wordpress″;

- Розміщувати свої проекти на якісних хостінгах;

- Не замовляйте розробку інтернет-проектів у людей, які пропонують малу ціну за роботу.

Ретельне дотримування цих рекомендацій зменшить ризики та покращить захищеність інтернет-проектів користувачів, створених на платформі ″Wordpress″.