УДК 004.9
Швед Х. – ст. гр. СНм – 51
Тернопільський національний технічний університет імені Івана Пулюя

ВРАЗЛИВОСТІ ВЕБ-СЕРВЕРІВ

Науковий керівник: асистент Маєвський О. В.

Коли мова заходить про уразливість веб-серверів, то переважна більшість людей відразу ж згадують «дірки» в їх програмному забезпеченні. Це відноситься до самих програм-серверів, таких як Apache, Microsoft Internet Information Server і т. д. І в цьому немає абсолютно нічого дивного. Все-таки це програмне забезпечення досить об'ємне і складне, так що «дірки» в ньому обов'язково є. Крім того, не можна забувати, що сучасний веб-сервер неможливо уявити собі без багатьох додаткових функцій, наприклад без підтримки мов програмування типу Perl, PHP і т. д., а також без систем управління базами даних. Все це стає можливим завдяки установці на веб-сервер додаткового програмного забезпечення.

Головною особливістю виробничих вразливостей є їх прихильність до певних версій програмного обеспеченія. Справа в тому, що «дірки» часто зустрічаються не у всій лінійці веб-серверів, а тільки в деяких їх релізах. Захиститися від даного типу вразливостей програмного забезпечення можна тільки одним способом - своєчасною установкою всіх розроблених виробниками оновлень. Вразливості можуть виникати через некоректне налаштування програмного забезпечення веб-сервера.

Напевно, ні для кого не секрет, що безпека будь-якої речі залежить від того, як її застосовувати. Те ж саме можна сказати і про веб-сервер. Дуже багато залежить від того, як налаштоване його програмне забезпечення. Взагалі, переважна більшість веб-серверів мають досить великий набір параметрів, що стосуються практично всіх аспектів їхньої діяльності. Таким чином, безпека багато в чому залежить від адміністраторів, що займаються їх обслуговуванням.

Від некоректного налаштування не може допомогти установка оновлень. І дійсно, при оновленні програмного забезпечення його конфігурація не змінюється. А це означає, що уразливість в системі захисту після інсталяції оновлення швидше за все залишиться. Таким чином, головною небезпекою розглянутого типу «дірок» є складність їх виявлення. Отже єдиний спосіб дійсно надійного захисту від таких вразливостей-використання спеціальних сканерів безпеки. Ці програми за допомогою спеціальних методів досліджують захист веб-серверів і знаходять всі потенційно небезпечні місця.

Скрипти веб-сайтів теж можуть містити вразливості. Сучасний веб-сервер і супутнє програмне забезпечення дуже часто служать своєрідною базою для виконання програм, які написані власноруч користувачем. Мова йде, звичайно ж, про скрипти, які працюють на більшості сучасних сайтів. Справа в тому, що більшість мов веб-програмування є серверними. Це означає, що скрипти, написані на них, виконуються прямо на сервері, а на комп'ютер користувача (в даному випадку - відвідувача сайту) відправляються тільки результати їх роботи. В даній ситуації криється досить серйозна небезпека. Справа в тому, що скрипти для сайтів далеко не завжди розробляються дійсно хорошими спеціалістами. На багатьох веб-проектах використовується безкоштовне програмне забезпечення. Природно, у ньому теж можуть міститися уразливості. Причому деякі з них можуть бути дуже серйозними, що дозволяють зловмисникам отримати несанкціонований доступ до самого сервера. Причому потрібно враховувати, що деякі скрипти виконуються з підвищеними привілеями.