Класифікація вразливостей Web-ресурсів

Войтович О.П.[1], Ювковецький О.С.[2]

[1]К.т.н., доцент кафедри захисту інформації, Вінницький національний технічний університет
вул. Хмельницьке шосе 95, м. Вінниця, Україна, voytovych.op@gmail.com
[2]студент кафедри захисту інформації, Вінницький національний технічний університет вул. Хмельницьке шосе 95, м. Вінниця, Україна, alexyuvkovetskyi@gmail.com

***Анотація* — Існуючі вразливості Web-ресурсів ставлять під загрозу нормальну роботу інформаційно-комунікаційних систем. Для покращення їх ідентифікації запропоновано класифікацію вразливостей Web-ресурсів, яка забезпечує краще розуміння проблеми. Як критерії обрані ознаки, що характеризують як загальні риси вразливостей, так і специфічні. Визначено якісні характеристики конкретних вразливостей, по яким ці вразливості і класифіковано.**

Ключові слова: Вразливість Web-ресурсів, Web-додатки, класифікація вразливостей Web-ресурсів.

Classification of Web-resources vulnerabilities

Voytovych O.P.[1], Yuvkovetskyi O.S.[2]

[1] Ph.D., associate professor of Information Security Department, Vinnytsia National Technical University
Khmelnytske shosse str., 95, Vinnytsia, Ukraine, voytovych.op@gmail.com
[2] Student, Information Security Department, Vinnytsia National Technical University
Khmelnytske shosse str., 95, Vinnytsia, Ukraine, alexyuvkovetskyi@gmail.com

***Abstract* — Existing vulnerabilities of Web-resources threaten the regular work of information systems. To improve the identification process, classification system of vulnerabilities of Web-resources, which will provide the better understanding of this problem, was proposed. General features as well as the specific details of the vulnerabilities were chosen as criteria. Vulnerabilities are classified by using the qualitative characteristics which were defined.**

Keywords: Web-resources vulnerabilities, Web-applications, classification of Web-resources vulnerabilities.

I. Вступ

Більшість Web-ресурсів не відповідають сучасним вимогам безпеки. Вразливості Web-ресурсів можуть поставити під загрозу імідж, фінанси, активи, персональні дані та інші цінні ресурси організацій, а отже як підсумок банкрутство або повна ліквідація компанії.

Метою даної роботи є виявлення класифікаційних ознак вразливостей Web-ресурсів, які б дозволили полегшити аналіз безпеки.

На сьогоднішній день існує велика кількість як ієрархічних, так і не ієрархічних класифікацій [1], які систематизують різні види вразливостей та атак, що на них базуються, за різноманітними параметрами. Розглянуто такі класифікації як OWASP [2], систематику Маркова [3], реєстр вразливостей CAPEC, класифікацію загроз WASC [4], модель загроз Microsoft STRIDE та класифікацію лабораторії Касперського [5]. У цих та інших джерелах описані основні вразливості Web-ресурсів та атаки на них. Але в них фактично відсутні класифікаційні ознаки, які б дозволяли універсалізувати виявлення та ідентифікації вразливостей. Подібні класифікації виділяють лише класи вразливостей, описані у загальному вигляд [3,4] або з деталізацією без загальних рис [2, 5]. Однак, ці класифікації є основою для побудови моделей вразливостей інформаційної безпеки.

Враховуючи досвід існуючих класифікацій, визначено і сформульовано основні вимоги для створення класифікації, яка базується на різних аспектах Web-ресурсів, а також виникненні конкретної вразливості у певний момент циклу роботи.

II. Критерії класифікації вразливостей

Класифікація вразливостей Web-ресурсів дозволяє ідентифікувати певну вразливість. Завдяки тому, що класифікація структурована за різними етапами [6], вразливості можуть бути розглянуті у будь-який момент життєвого циклу Web-ресурсу, враховуючи мету зловмисника, розташування жертви, спосіб впливу на систему, тощо. Це дозволить покращити захист конкретного Web-додатку від атак зловмисників.

На рис. 1 наведено запропоновану класифікацію вразливостей Web-ресурсів.

Розглянемо кожну з класифікаційних ознак. **За ступенем автоматизації** вразливості поділяють на ручні (R1), напівавтоматичні (N1) та автоматичні (A1). Якщо говорити про напівавтоматичні та автоматичні вразливості, то їх в свою чергу також поділяють на кілька підвидів:

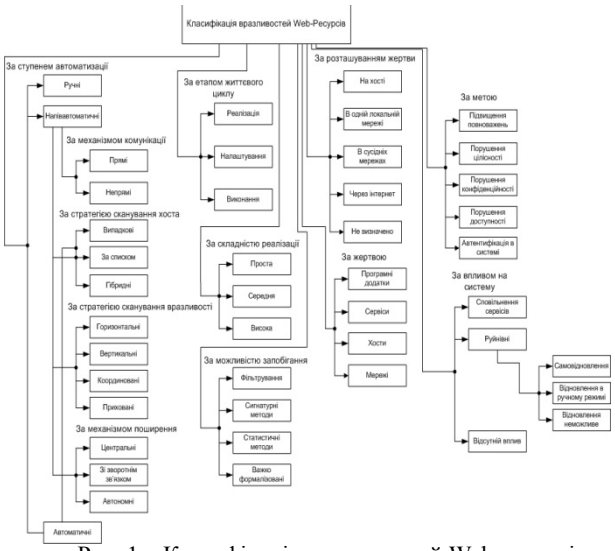

Рис. 1 – Класифікація вразливостей Web-ресурсів

За механізмом комунікації виділяють прямі (P11) та непрямі (N11).

За стратегією сканування хоста - випадкові (V12), за списком (V22), гібридні (V32).

За стратегією сканування компонентів - горизонтальні (G13), вертикальні (V23), координовані (K33), приховані (P43).

За механізмом поширення - центральні (C14), автономні (A24), зі зворотнім зв'язком (Z34).

Також вразливості класифікують **за етапом життєвого циклу**, на якому вони виникають. Розрізняють три основних етапи: реалізація (R4), налаштування (N4) і виконання (V4).

За складністю реалізації вразливості. Вразливості, які можна реалізувати без втручання у саму систему називають простими (P5). Середній рівень складності (S5) – це вразливості, використання яких потребує моніторингу для пошуку дірок у системі. Складною реалізацією (Sk5) називають випадки, коли для використання вразливостей необхідно порушувати нормальну роботу системи.

За можливістю запобігання вразливостям розрізняють наступні види: фільтрування (F6), використання сигнатурних методів (S6), використання статистичних методів (St6), використання важко формалізованих задач (VF6).

За метою зловмисника, жертвою можуть стати наступні компоненти: програмні додатки (P7), сервіси (S7), хости (H7), мережі (M7).

За розташуванням жертва може знаходитись на хості (H8), в одній (O8) або сусідніх (S8) зі зловмисником локальних мережах або на зв'язку через інтернет (I8). Бувають випадки, коли визначити розташування зловмисника відносно жертви неможливо (N8).

За метою використання вразливостей можна розділити на наступні категорії: порушення конфіденційності (K9), порушення цілісності (C9), порушення доступності (D9), підвищення повноважень (P9), автентифікація в системі (A9).

Також одним із дуже важливих факторів є **вплив на систему**. Використання деяких вразливостей не чинить впливу на систему (N10), інші ж сповільнюють сервіси (S10). При використанні деяких вразливостей вплив може бути руйнівним (R10). За такого впливу відновлення систем може бути наступним: самовідновлення (S109), відновлення у ручному режимі (R210), відновлення неможливе (N310).

На прикладі вразливості **CSRF** (англ. Cross Site Request) покажемо спрощену ідентифікацію цієї вразливості Web-ресурсів, яка базується в тому числі на недоліках протоколу HTTP. Атака здійснюється шляхом розміщення на Web-сторінці посилання або скрипта, який намагається отримати доступ до сайту, на якому знаходиться користувач-жертва. Додаток дозволяє користувачеві відправити запит на зміну стану, що не включає в себе нічого секретного.

```
http://example.com/app/transferFunds?amount=1500&destinationAccount=46732432
```

Зловмисник створює запит, який буде переводити гроші з рахунку жертви, а потім вбудовує цю атаку в запит зображення, що зберігається на різних об'єктах, що знаходяться під контролем зловмисника.

```
<imgsrc="http://example.com/app/transferFunds?amount=1500&destinationAccount=
attackersAcct#" width="0" height="0" />
```

За ступенем автоматизації ця вразливість ручна (R1). За етапом життєвого циклу, на якому виникає подібна вразливість: реалізація (R4) та налаштування (N4). За складністю реалізації – середня (S5), так як зловмиснику необхідно проаналізувати Web-ресурс на помилки конфігурації та недостатню фільтрацію вхідних даних. За стратегією сканування – приховані (P43). За можливістю запобігання – фільтрування (F6). Метою є сервіс (S7). Розташування жертви тут не визначено (N8), хоча в основному подібні атаки проводять через Інтернет (I8). За метою – підвищення повноважень (P9) та порушення цілісності (C9). Вплив на систему при атаках такого типу відсутній, робота сервісу не порушується (N10).

III. Висновки

Отже досліджено відомі класифікації вразливостей Web-ресурсів.

Запропонована класифікація вразливостей Web-ресурсів, яка може стати корисною при розробці інструментів аналізу безпеки Web-ресурсів.

В подальшому планується продовжити дослідження в напрямку збільшення ознак, які можуть бути використані.

[1] СТАТИСТИКА УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ 2012 [Електронний ресурс]. – Режим доступу:URL: http://ptsecurity.ru/download/analitika_web.pdf - Назва з екрану.

[2] 2013 Top 10 Vulnerabilities List [Електронний ресурс]. – Режим доступу:URL: https://www.owasp.org/index.php/Top_10_2013-Top_10 - Назва з екрану.

[3] А.С. Марков, А.А. Фадин - Систематика уязвимостей и дефектов безопасности программных ресурсов [Електронний ресурс]. – Режим доступу:URL: http://www.npo-echelon.ru/doc/is_taxonomy.pdf- Назва з екрану.

[4] " Common Web Application Vulnerabilities" [Електронний ресурс]. – Режим доступу:URL: https://cve.mitre.org/- Назва з екрану.

[5] "Защита от эксплойтов в Антивирусе Касперского" [Електронний ресурс]. – Режим доступу:URL: http://www.kaspersky.ru/downloads/pdf/technology_auto_protection_from_exploit.pdf/ - Назва за екрану.

[6] A Taxonomy of DDoS Attackand DDoS Defense Mechanisms [Електронний ресурс]. – Режим доступу:URL: http://www.eecis.udel.edu/~sunshine/publications/ccr.pdf/ - Назва з екрану