Драган Д.Д., Поляков А.Ю. *— рецензент Кирюша Б.А.*
Інститут прикладного системного аналізу НТУУ "КПІ", Київ, Україна

Аналіз безпеки веб-порталу GRID ALLTED за допомогою засобів автоматизованого тестування

Звичайно аналіз безпеки веб-ресурсу потрібно проводити з самого початку роботи над ним, визначаючи потенційні загрози та можливу стратегію поведінки зловмисників і вчасно розроблюючи засоби протидії [1]. Такий аналіз на різних стадіях розробки включає наступні етапи:

- Аналіз документації та спілкування з розробниками стосовно мір безпеки системи;
- Моделювання можливих загроз, документування;
- Аналіз програмного коду;
- Тестування готової до використання системи в ролі атакуючого за допомогою
  1. засобів автоматизованого тестування (програм або фреймворків котрі проводять заданий набір тестів на вразливості в автоматичному режимі);
  2. вручну.

Інколи виконати повний цикл аналізу неможливо (наприклад, коли система вже знаходиться на фінальних фазах розробки). Тоді слід виконати тестування системи в ролі зловмисника (останній етап), яке також називають тестуванням за принципом «чорної скриньки», бо звичайно зловмисник володіє мінімумом інформації про внутрішній устрій системи. У такому разі технічні засоби (сканери уразливостей тощо) можуть зберегти багато часу та зусиль у пошуку можливих шляхів атаки, але, очевидно, слід визнати, що вони менш гнучкі та ефективні порівняно із спеціалістом високої кваліфікації, тому вони не претендують на повноту аналізу, а повинні використовуватися лише як його складова.

Результати. Наведемо основні результати виконання такого автоматизованого аналізу для веб-порталу GRID ALLTED (allted.com) за допомогою програмного забезпечення XSpider та JSky.

Табл. 1. Результати автоматизованого аналізу безпеки досліджуваного веб-ресурсу

Клас проблеми	Наявність на досліджуваному ресурсі
Cross-site scripting (XSS)	Наявні проблеми із низьким рівнем небезпеки
Bruteforce (отримання паролю при наявному логіні)	Наявна проблема із низьким рівнем небезпеки
Privilege escalation	Наявна проблема із середнім рівнем небезпеки
DoS (Denial of Service)	Наявна проблема із низьким рівнем небезпеки
Injection Flaws	Не виявлено
Broken Authentication and Session management	Не виявлено
Insecure Cryptographic Storage	Не виявлено
Cross Site Request Forgery (CSRF)	Не виявлено
Information Leakage and Improper Error Handling	Значних проблем не виявлено
Failure to Restrict URL Access	Не виявлено
Insecure Direct Object Reference	Не виявлено
Insecure Communications	Не виявлено
Malicious File Execution	Не виявлено

Висновки. Було виконано аналіз деяких уразливостей веб-порталу GRID ALLTED та запропоновані шляхи їх нейтралізації. Подальша робота в цьому напрямку передбачає усунення наявних проблем.

Література. **1.** Open Web Application Security Project testing guide [Електронний ресурс]. - Режим доступу: http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf