xHunter: Tracking XSS on the Net

The exploitation of web applications has become a major threat for every user that performs daily activities in the world wide web. The research and academic community is heavily involved in exploring new techniques for protecting web applications, and thus the users, from web attacks. However, we still know little about real-world incidents regarding web exploitation. In this project, we design and implement xHunter, a detector that is able to analyze URLs, which can exploit web applications. Using xHunter we can analyze web attacks that have been already reported to security vendors, we can investigate the web sites that are targets of web attackers, the time it takes for a web vulnerability to be fixed, the growth of web reports, and other properties that assist in getting a finer-grained picture of web exploitation. Finally, xHunter can be deployed in a live network for detecting attempts based on XSS exploitation, and thus can be used to protect users from XSS exploitation.

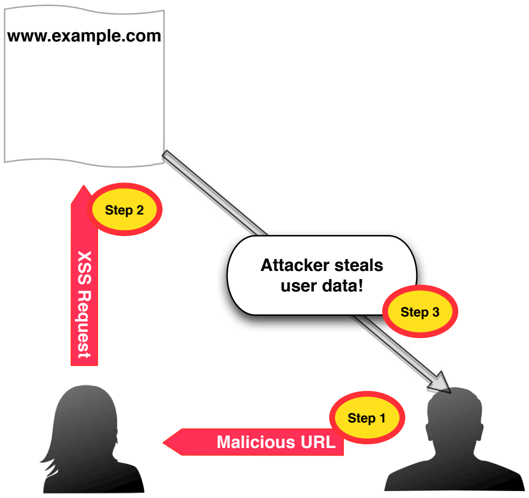

Figure 1: The XSS problem in three steps. In Step 1, the attacker sends a *special* (malicious) URL to the victim. In Step 2, the victim, by opening the attacker's URL, performs a request to a legitimate web site. Finally, in Step 3, the attacker steals the victim's data (e.g., e-banking credentials).

Problem and Impact

The timing between identifying an XSS attack (see Figure 1 for an illustration of XSS) and resolving it is crucial. According to a study on the Cost of Cyber Crime, by the Ponemon Institute, the average time it took to resolve a cyber attack was 32 *days – with an average cost of $1,035,769 (that's $32,469 per day) for the participating sample of organizations.* [1]

xHunter

xHunter can be a useful tool against web exploitation. It can operate in the following modes:

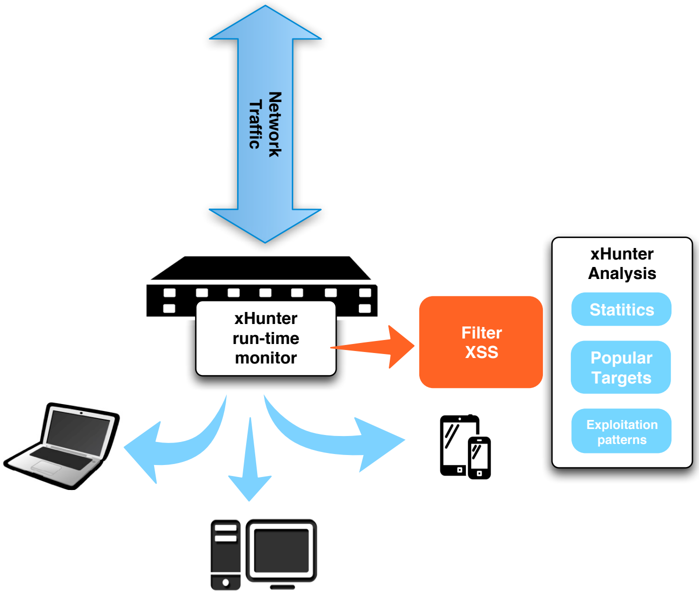

Figure 2: The architecture of xHunter. It can both act as a run-time monitor for filtering out dangerous traffic (XSS URLs), as well as an off-line analysis framework for analyzing web exploitation based on XSS.

- **On-line detector:** xHunter can process in real-time incoming URLs and infer if they aim at exploiting web applications. In that sense, xHunter can form a custom, and more sophisticated, firewall, which is able to comprehend XSS exploitation and prevent it. xHunter can be an important element of the security infrastructure which shields a modern web server and its role should be very important, especially if we take into account the popularity of XSS exploitation nowadays.
- **Off-line analyzer:** xHunter can be used for analyzing collected URLs offline. In this mode, xHunter can be a useful tool to the security analyst, since it can assist in characterizing a large group of malicious URLs and infer many insights about how attackers try to exploit web applications.

The two modes of operation of xHunter are illustrated in Figure 2.

[1] More information at: https://www.acunetix.com/blog/articles/return-on-investment-protecting-cross-site-scripting/.