Injecting malicious script through links, URLs (Unified resource locator) or as user inputs and getting it executed (when inputs are not validated) in the client side is called cross site scripting (XSS) attack. It is called XSS because the script that is executed here is not originated from the same client or from a trusted server. Our solution “Yukti” is devised to detect these application specific XSS attacks at network level by deep packet inspection in the live environment. Existing solutions do static security code review or scans the application for known attack patterns. “Yukti” is dynamic as the suspect engine in the solution is unique and has the capability to suspect a new attack pattern. If the suspect is analyzed to be true, the rule that would detect the attack is built into rule base dynamically. This paper discusses the design, components, architecture, dependencies, techniques, implementation and analysis of results obtained. Our results show that out of huge test cases (70000- both XSS and Non XSS) the solution is able to detect 28546 numbers of XSS attacks initially (before appending new rules in detection engine). After appending new rules based on recommendations from suspect engine, it is able to detect...
32363 XSS. Yukti demonstrates considerable improvement in the performance when analyzed with leading IDS engine SNORT while detecting XSS attacks.

Reference

- P.Vogt, “Cross Site Scripting (XSS) attack prevention with dynamic data tainting”, 2006
- M.Egele, M.Szydlowski, E. Kirda, and C. Kruegel,”Using Static Program Analysis to Aid Intrusion Detection”, Austrian Science Foundation (FWF) under grant P18368-N04
- Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications that enables attackers to inject client-side script into Web pages viewed by other users. http://en.wikipedia.org/wiki/Cross-site_scripting
- National Vulnerability database http://nvd.nist.gov/
- Whois lookup, domain name search, domain name registration, available domain names, domain whois database information. www.whois.com
“Yukti”: A Dynamic Agents Based IDS with Suspect Engine to Detect Diverse XSS Attacks

- jpcap -- a network packet capture library for applications written in Java.
  http://jpcap.sourceforge.net/
- Sourcefire Vulnerability Research Team™ (VRT) Rules are the official rules of snort.org.
  https://www.snort.org/snort-rules

Index Terms

Computer Science

Security

Key words

Cross Site Scripting  XSS

Web

Application Security

Application Intrusion Detection

Security Attacks

Vulnerability Management