YOUNKER YSCANNER OVERVIEW

Web Application Scanner

Vulnerability Scanning System

CATALOGUE

1. Challenges

■ Challenges of source code

Web application systems are typically customized by vendors for different business goals, delivered as "source code", and dynamically parsed by a variety of application environments to achieve specific functionality. Therefore, suppliers is often difficult to provide general patch, the Web application system maintenance has brought new challenges - not just rely on the passive way of "patch", and the needs to adopt a more active way, using professional Web vulnerability scanning system to evaluate, discover hidden vulnerabilities in Web application system in advance, according to the assessment tool gives detailed bug description and repair plan, guide the maintenance personnel on security reinforcement, nip in the bud.

■ Another challenge introduced by routine inspection task

Safety inspection tasks are often time-consuming and heavily, especially for those increasingly large scale site, a single site always hosts thousands or even tens of thousands of pages, and also security check have to deal with more than one site, at the same time, with the constantly emerging of the new web technologies, the structure of the site is becoming more and more complex, so how to conduct quickly and stable scanning is growing to be a bigger problem to be solved.

2. Product Introduction

Rather than relying on those public vulnerability libraries, our detection is aimed at unknown Web application vulnerabilities. The formers are based on third-party vulnerabilities and their tests, most of which are public vulnerabilities, have been used

for test on bugs. While, web application vulnerabilities, which are derived from those bugs that the web app developers have introduced during the course of coding stage, are the vulnerabilities of the web application itself, and the detection of this type of vulnerabilities, can't be relied on public vulnerabilities, and should be detected through specialized web applications that challenge against products being tested through a specific algorithm.

Our YScanner - vulnerability detection professional scanning tools, fully supports OWASP TOP 10 detection, based on the latest browser engine technology and powerful crawler, rich variety of accurate detection algorithms, has an absolute competitive advantage in the omission rate and false alarm rate. Moreover, due to development based on Linux system and without being limited by by Windows copyright, hence provides Linux innate higher performance and larger concurrency advantages. It supports the detection of a very hidden storage XSS flaw in the second XSS flaw of OWASP Top 10. Especially, in comparison with current products existing in the market, YScanner needs unsupported maintenance or limited supports.

3. Core competitiveness

The core competitiveness of YScanner - vulnerability scanning system mainly focus on:

- **The reptile's crawling ability is the basic guarantee of low FRR.**

The crawler likes person’s eyes, meanwhile, the vulnerability detection algorithm looks like the sword in hands. YScanner is independently developed based on the latest browser engine technology, its crawling ability is at the cutting edge in this sector of cyber security market. WIVET is a national standard test project to assess crawl capability, in 2016 testing, within global mainstreams recommended web application vulnerabilities detection products, including HP Webinspect, famous WVS and IBM Appscan (Top 3 vendors, their crawl coverage rate reached to 96%, 94% and 92%, respectively), YScanner achieved 96%, the same as HP’s Webinspect.

- **YScanner uniquely constructs the diversified and accurate detection algorithms mechanism**

The detection on many vulnerabilities even reaches to zero false positive rate. For example, the XSS vulnerability ranked no. 2 by OWASP, currently such tools are generally based on the detection technology of pattern recognition, and easily lead to false positives and does not support Stored XSS detection. YScanner leverages browser sandbox technology to detect XSS vulnerabilities. It not only supports conventional XSS vulnerability detection, but also provides strong support for Stored XSS and DOM XSS meanwhile, zero false alarm rate is kept.

- **Strong authentication scanning capability**

Our web application scanning system is based on the independently developed crawler and browser plug-in technology, has a strong automatic identification ability for login form, and furthermore, authentication with verification code is also ben strongly supported.

- **Combining browser plug-in technology and crawler technology**

Security analysis can be carried out for all HTTP traffic during functional testing, hence can dig deeper into the vulnerabilities of web applications.

- **Linux-based system**

Without limitation of Windows copyright and performance, performance is an inherited advantage from Linux platform。

- **Strong cloud deployment capability**

Just from the beginning of architecture design stage, YScanner took into account the supports of cloud computing, which not only has a strong cloud deployment ability, but also provides a very convenient interface and flexible scalability. With the aid of scanning system, Enterprises can easily build their own security capability in private clouds. We also provide SaaS solution, a public cloud platform integrated with YScanner, conduct remote Web security scanning, Enterprises can log into the public cloud platform, and get remote security evaluation of their website or web application

system.

4. System functions

4.1 System architecture

YScanner mainly consists of two parts: security detection platform and scanning engine:

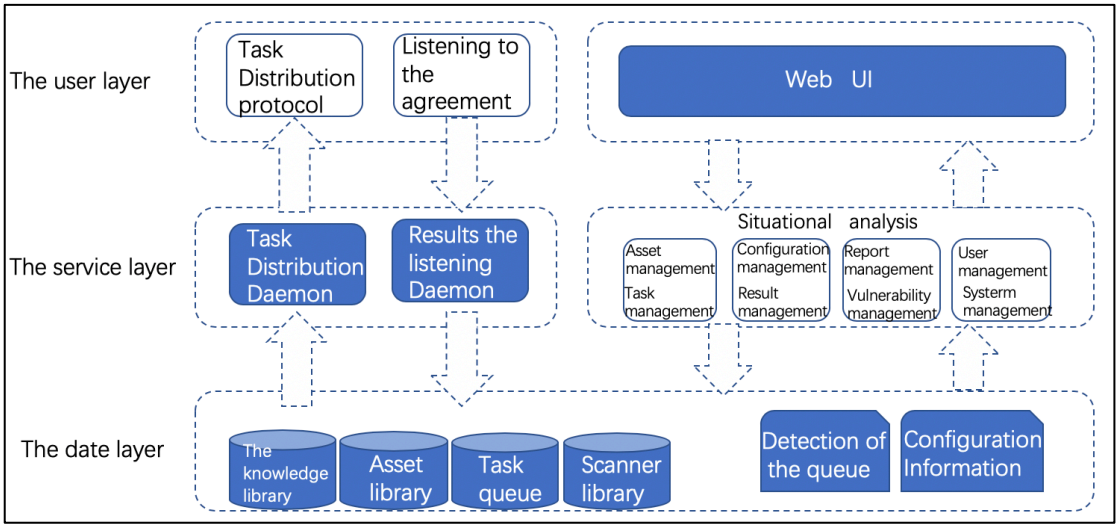

Fig. 1 System architecture of vulnerability scanning and detecting platform

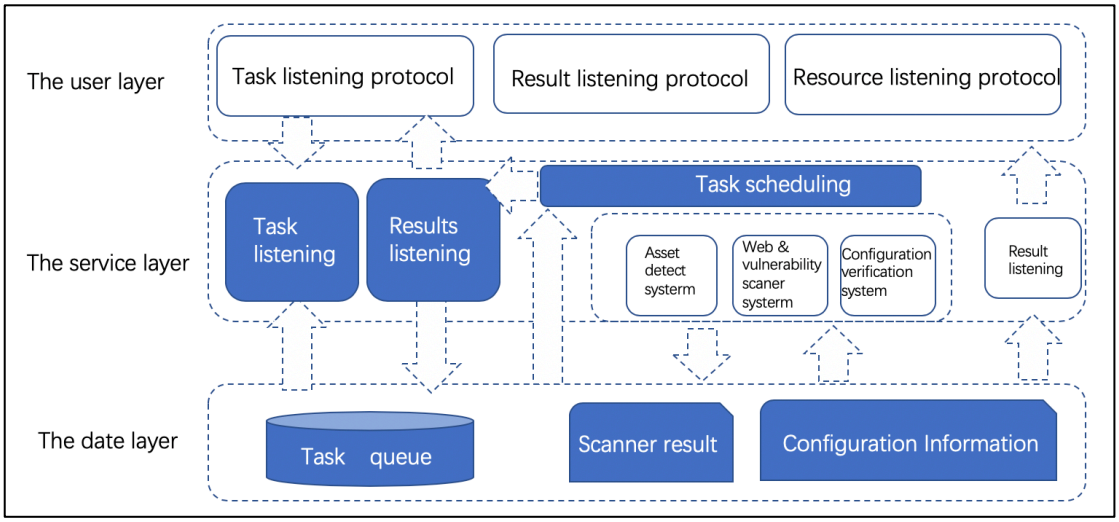

Fig. 2 Architecture of vulnerability scanning engine

4.2 Product functions

➢ Powerful vulnerabilities matching

Full support for OWASP top 10, by the WASC standard classification, supporting on web application vulnerabilities are the most thorough and the most granular. User can freely select from the portfolio, or it can be directly settled for entirely chosen or not.

➢ Flexible scanning resolution

All kinds of dynamic content checking is supported, including all kinds of javascript , JS framework, flash, and so on, provides the most thorough and powerful analytical capability, moreover, YScanner keeps a long detailed history of Web applications.

➢ A thorough and detailed deep scan

With the above two capabilities, security analysis can be performed for all HTTP traffic during functional testing, which helps on digging deeper into the vulnerabilities of web applications.

➢ Log check and certification

On every vulnerability being detected, YScanner provides vulnerability verification interface to facilitate users to verify relating vulnerability; scanning log will be provided for user to monitor scanning authentication results and scanning progress; all pages will be scanned, also supports the generation of site directory tree; as for authentication results, the snapshot function is developed for user to sense the real result of authentication with the aid of the snapshot contents. If the real result is failure, it can help to understand the cause of authentication failure, moreover, to set the authentication correctly.

➢ Supports multiple authentication scanning

YScanner supports authentication on user name and password based and session-based, also owns the ability of automatically capture Session.

➢ Flexible, simple, professional scanning customization

More granular scanning settings are available, such as:

- Scanning configuration template management function
- Single user and multi-user concurrent scanning
- Scanning path setting
- Scanning blacklist setting
- Header injection scanning configuration

5. Features

5.1 Strong ability of dynamic analysis

With the development of Web technology, Web content has gone from static pages to dynamic pages with the rich content. The analysis of dynamic content generated by various dynamic codes in response pages is a challenge that faced by Web application vulnerability detection technology. The ability of dynamic analysis, as well as the type and depth of dynamic code support, is one of the key factors to evaluate the vulnerability scanning system, otherwise, higher failure rate will naturally occur.

The deep scanning intelligent engine of YScanner system hence provices very powerful dynamic analysis capability. It can comprehensively and accurately analyze Javascript code, various JS framework code, Flash code in response pages, etc., and it also overcomes the difficulties of technical analysis in JQuery code. This greatly strengthens the crawling and vulnerability mining ability of YScanner, and furthermore ensure extremely low FRR.

5.2 Rich detection algorithms

The traditional detection method based on vulnerability database signature is applicable to known vulnerabilities, i.e., the detection of vulnerabilities depends on

library size and publicly update frequency, however, there has nothing to be do for the "unknown threats" that have not been disclosed. The former approach is effectively and applied to operating systems, databases, middleware, and server-like software (e.g. Apache), as well as to the framework programs used by web applications, however not applicable to a vast, diverse and complex web applications.

Traditional web application vulnerability detection algorithms usually adopt conventional detection method similar to vulnerability library signature, which is simple to implement, owns strong applicability for different web application vulnerabilities, and is easy to maintain, but has higher alarm failure and false alarm rate. In order to ensure the detection and accuracy of web application vulnerability inspection, YScanner combines the strength of conventional vulnerability inspection method and new evolving technology in this aspect, then builds a newly detection mechanism and relevant algorithms, hence, realize lower false alarm rate and FRR. Especially, in the mining of storage XSS vulnerabilities and DOM-based XSS vulnerabilities.

5.3 The unique omission of the error report analysis capability

In addition to affection results from the dynamic analysis and detection algorithm, Web application vulnerabilities detection accuracy is also affected by some outside interference factors, such as the interference of WAF firewall, in some cases, false positives are caused by heavy network traffic and server load, and a timeout or gateway error caused by the omission or mis-statement. How to suppress these external interference factors with improvement on the detection accuracy, this is another bigg challenge. YScanner optimizes its architecture and algorithms on the above aspect, introduces a new specific analysis, and provide special reports to disclose the possible omission and false positives to security engineers

5.4 Powerful ability on login form automatic recognition

The automatic identification ability of login form is also one of the key strengths of YScanner, which determines the degree of automation of the vulnerability detection process. With a simple username and password, the detection system can automatically recognize the login form and complete the complex login process, which is obviously easier to implement than other methods (e.g. recording, cookie-based authentication, etc.)

YScanner relies on its underlying intelligent engine and extra powerful ability to automatically identify login forms, hence, in most cases, the scanning task can automatically identify and complete the login process simply by providing the login account and password. Also, simply configuring a few items on the scan configuration/basic options page below will launch a scan successfully

5.5 The most extensive web application vulnerability support

In terms of identifying vulnerabilities introduced by web application developers in coding, YScanner is currently the most supported scanning system in the domestic market

It also supports the vulnerability detection of third-party code introduced by the framework program integrated by Web applications, and it also has good support for the limited vulnerability scanner of many Web applications, which is introduced by coding.

5.6 Highly competitive low FRR and low alarm rates

Strong dynamic analysis capability and rich optimal detection algorithms ensure YScanner owns a very low FRR and false alarm rate, which shows better practical rate on the spot than same types of the products.

More information
visit our website https://www.yscanner.com/index.html

Beijing Yuanhe technology co., ltd.

Block C, Room 603, Wanlin Science and Technology Building,

No.8 Malianwa North Road

Haidian District, Beijing

+86-10-527-14369

E-mail: security@yuanhetech.com