International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 777-781www.ijaem.net ISSN: 2395-5252

Web Vulnerability Scanner using ModifiedCross Script Algorithm

Hrushikesh Panchbudhe
Student, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, Maharashtra
Student, Tulsiramji Gaikwad-Patil College of Engineering and Technology, Nagpur, Maharashtra
Guide: Prof. Anup Gade, Co Guide: Prof. Vijay Bagdi

Submitted: 05-03-2021 Revised: 18-03-2021 Accepted: 20-03-2021

ABSTRACT: We use numerous websites in our day to day life. But we are unaware of the attacks happening on these websites. To protect our websites from those attacks we are creating a tool that will give us solutions to overcome these attacks. The last few years has shown a high increase in the number of web-based attacks. There are various vulnerabilities but SQL injunction and cross-site scripting is the main. All the websites on the internet may get affected due to these attacks. Although the bulk of web vulnerabilities are easy to know and to avoid, many web developers are, unfortunately, not security-aware. As a result, there exist many internet sites on the web that are vulnerable.
This project implemented an automatic vulnerability scanner for injection attacks. In this project, we have created a scanner application that will give us the solution for these attacks and it will also help us to know how strong the website is so that it doesn't get hacked. Our system automatically analyses web sites to find exploitable SQL injection and XSS vulnerabilities. It can find many potentially vulnerable web sites.

I. INTRODUCTION

Security is a critical part of your Web applications. Web applications by definition allow users access to a central resource — the online server — and thru it, to others like database servers. The vulnerability may be a hole or a weakness within the application, which may be a design flaw or an implementation bug that permits an attacker to cause harm to the stakeholders of an application. Stakeholders include the appliance owner, application users, and other entities that rely on the application. The term "vulnerability" is often used very loosely.

Web Security blocks web threats to scale back malware infections, decrease help desk incidents, and release valuable IT resources. It has quite 100 security and filtering categories, many web application and protocol controls, and 60-plus reports with the customization and role-based access. You can easily upgrade to Web Security Gateway when desired to urge social media controls, SSL inspection, data loss prevention (DLP) and inline, real-time security from Web sense ACE (Advanced Classification Engine).

Development of Scanner for detecting vulnerabilities to
Guard the web site from web-based attacks.
OWASP top 10 Web Application Security Risk (2017)

- A1 - Injection
- A2 - Broken Authentication
- A3 - Sensitive Data Exposure
- A4 - XML External Entities
- A5 - Broken Access Control
- A6 - Security Misconfiguration
- A7 - Cross-Site Scripting
- A8 - Insecure Deserialization
- A9 - Using components with known vulnerabilities
- A10 - Insufficient logging and Monitoring

II. LITERATURE SURVEY

A. Review:

The rapid and tremendous growth of Information and Communication Technology (ICT) has increased access to web applications. This increased access has paved the way for disadvantageous security and vulnerable threats in the form of attacks in web applications. Various detection and prevention techniques are proposed by researchers within the field of web applications and technology development. Through relevant literature and existing research presents a viewpoint of different web application vulnerabilities and security threats and also outlines some open research issues under the state-of-the-art.

The following diagram depicts these security layers as a holistic outlook that appears at security as hardened measures taken to attenuate intrusion risks and maximize the protection of the key asset of any organization, its data.

B. Vulnerabilities distributed per type:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 777-781www.ijaem.net ISSN: 2395-5252

Figure 2.2 presents the ultimate distribution of vulnerabilities per type including the doubtful cases (i.e., optimistic evaluation of the scanners). As the doubtful cases only affect the SQL Injection, it means the amount of SQL injection vulnerabilities might be overestimated. Scanners have found 177 different vulnerabilities in 25 different services, which imitate approximately 8.33% of the tested services. As mentioned before, the potent vulnerability is SQL Injection, representing 84.18% of the vulnerabilities found. This is a really important observation thanks to the high number of cases found and therefore the high severity of this vulnerability.

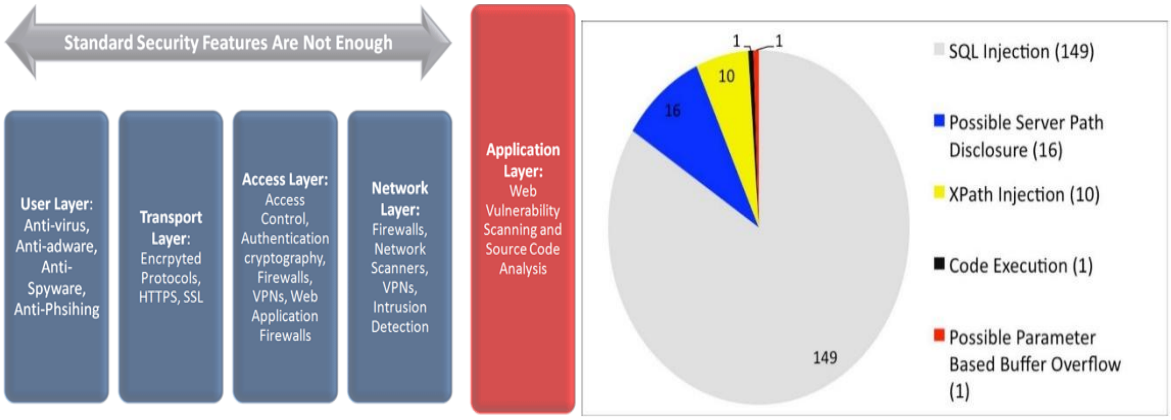


Fig 2.1 Security Layers as a Holistic OutlookFig 2.2 Pie Chart of Web Application Vulnerability Statistics 2010-2013

Since 3 years the following trends have been observed:

• A steady decline in input validation weaknesses has been observed, for instance, Cross-Site Scripting affected 69% of applications in 2010, 66% in 2011, and 56% in 2012. Equivalently, SQL Injection concerned around 17% of applications in 2010 and 2011 and 15% of applications in 2012.

Context believes that our clients are getting more conscious of the risks posed by these issues, and are implementing more robust data validation controls within applications and integrating these controls into the development lifecycle.

• Topping the typical number of OWASP Top 10 issues in 2012 is once more "Broken Authentication and Session Management". This generic category includes an outsized number of the problems we identify; however, these sometimes overlooked issues are fundamental to the safety of web applications.

Server misconfiguration and information-leakage vulnerabilities have been the most prevalent Context technique category of issues identified in 2010, 2011, and 2012. This observation accentuates a possible disconnect between robust application development and secure deployment of applications into production environments

1. Abdul Razzaq, Ali Hur, Sidra Shabaz, Mudassar Masood, H Farooq Ahmad, Critical analysis on Web Application Firewall (2013) Critical analysis on Web Application Firewall: compared the Web Application Firewall (WAF) solutions with important features necessary for the safety at the application layer. Critical analysis on WAF solutions is useful for the users to pick the foremost suitable solution to their environments.

2. Wu Qianqian, Liu Xiangjun Research and Design on Web Application Vulnerability Scanning Service (2014) Scan approach to the web application firewall. The paper focuses on research among the existing Web application scanners essentially. Then we selected W3af (Web Application Attack and Audit Framework) as a basic platform for transformation, and by customizing scanning modules and scripts, we designed an internet application security scanning service.

3. Z.Ghanbari, Y. Rahmani, H. Ghaffarian, M. Hossein Ahmadzadegan Comparative approach to web application firewall (2015) Comparative approach to web application firewall: One of the newest tools to prevent infiltration and attacks on websites, are web application-specific firewalls or the online Application Firewalls (WAF) by which security policies are often applied among end-users and web applications. In this paper this feature has been implemented in software for cover and provides the advantage of preserving the safety in web applications against attacks and methods which affect the system together through a comparative approach.

4. Sajjad Rafique, Mamoona Humayun, Bushra Hamid, Ansar Abbas, Muhammad Akthar, Kamil Iqbal Web Application Security Vulnerabilities Detection (2015) A Systematic Mapping Study.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 777-781www.ijaem.net ISSN: 2395-5252

They planned to describe the mapping study for synthesizing the reported empirical research in the area of web applications security vulnerabilities detection approaches

5. IGN Mantra, Muhammad Alaydrus, HM Misni, The web security and vulnerability analysis model on Indonesia Higher Education Institution (2016) SQL injection, attacks, vulnerability analysis. The Sample Attacks which will be tested in sort of SQL injection to seek out vulnerabilities and supply prevention and countermeasures for the owner of the online site

6. OpenVas 9.0 (2017) Web Scanning Software OpenVAS is a full-featured vulnerability scanner.

7. Acunetix 11 2018 Online Scanning System Acunetix is one of the biggest players in the web security arena. The European-based company released the primary version of their product back in 2005, and thousands of clients around the globe use it to research the safety of their web applications. They recently unveiled Acunetix version 11, so we have decided to require it for a spin.

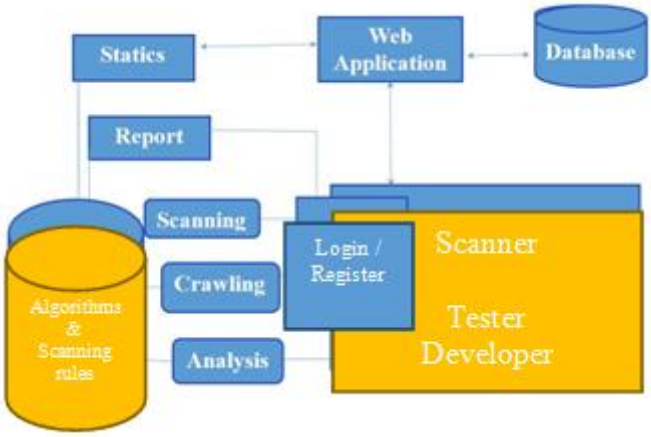
8. Bin Wang, Lu Liu, Feng Li, Jianye Zhang, Tao Chen, Zhewan Zou, Research on Web Application Security Vulnerability Scanning Technology 2019 Web crawler, XSS vulnerability, SQL injection vulnerability this paper studies the common web application security vulnerability scanning technology within the power industry Essentially, the working principle of vulnerability scanning is elaborated. Secondly, the specific vulnerability scanning technology is evaluated, and the implementation process of vulnerability scanning technology is emphasized. Finally, the key functions of the vulnerability scanning system are realized, and therefore the feasibility of the technology research is proved by the scanning results.

B. Problem Identified

This is aimed to fill the research gap between cyber security and web application. It presents a new technique to scan web application vulnerabilities. It is called a web vulnerability scanner. The target of new techniques is analyzing OSWAP vulnerabilities. This involves the removal of the data source. The proposed technique works on the removal of vulnerability and to provide appropriate solutions for those Vulnerabilities.

III. PROPOSED RESEARCH METHODOLOGY

3.1Existing Methodology:



3.1 Existing Methodology of Web Vulnerabilities Analysis

In the existing methodology, the web application is divided into several modules. It consists of a scanner, algorithms, reports, database, etc. Firstly, in the scanner module, the login/register functions will be performed. It includes the scanning, crawling, and analysis functions in the scanner module. Then both the module i.e. scanner and algorithm are connected to static, Report, and web application. All the data from the web application will get stored in the Database.

3.2 Proposed Work:

The scanner is going to take the URL of the website as input, to test for vulnerabilities as per the selected vulnerability. It will check whether the website exists in the domain or not. If not, it will ask the user to enter the correct website. It checks whether the web site exists or not by checking its status code. If the status code is 404 the URL does not exist. For a legitimate URL, it'll crawl the web site with the assistance of our own developed Crawler “basic crawler” basically made in Java. The Crawler will parse the website. The output of this phase is multiple frameworks, form details, and

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 777-781www.ijaem.net ISSN: 2395-5252

platforms used in developing web pages of the respective website. After parsing the web site, the Scanner will test all the forms and links of the web site for vulnerabilities.

The Scanner is scanning for two topmost vulnerabilities i.e. SQL Injection and Cross-Site Scripting. Both have different criteria

Table 1: Proposed Plan Work

Duration of Work	Action To Be Taken
Sep 2020	Literature review
Sep – Oct 2020	Publishing Review Paper & Implementing
Oct – Nov 2020	Implementing of another modulegroup feature selections
Nov – Dec 2020	Paper Publication on Problem Definition
Dec – January 2021	Classification of features
January – February 2021	Testing of Project
February – March 2021	Paper Publication on Result Analysis

IV. CONCLUSION

In this paper, our survey on detection and classification of cotton leaf disease using image processing and machine learning techniques was carried out. Also, the survey on background elimination and segmentation techniques was discussed. Through this survey, we concluded that for background removal color space conversion from RGB to HSV is useful. We also found that the threshold technique gives a good result as compared to other background removal techniques. We performed color segmentation by masking green pixels in the background removed image and then applying the Otsu threshold on the obtained masked image to get a binary image. This is very useful to remove accurate features of the disease. We searched that SVM gives good results, regarding the accuracy, for the classification of diseases. There are main five major steps in our present work, out of which three steps have been implemented: Image Acquisition, Image preprocessing, and Image segmentation. The remaining two steps are feature extraction and classification which we will implement in our future work.

REFERENCES

[1] Kevin J Vella, "The True Nature of Web Application Security: The Role Function of Black Box Scanners", IEEE, 21 Feb. 2007.
[2] Vieira, "Using Web Security Scanners to Detect Vulnerabilities in Web Services"; IEEE/IFIP Intl Conf. on Dependable Systems and Networks, Lisbon, Portugal, June 2009.(DSN 2009).
[3] Jan Tudor, "Web Application Vulnerability Statistics 2013"; IEEE June 2013.
[4] The 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks.(DSN2018).
[5] Conference Coordinator- The 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks.(DSN2016).
[6] 12th European Dependable Computing Conference.(EDCC2016).
[7] 7th Latin-American Symposium on Dependable Computing.(LADC2016).
[8] The 26th IEEE International Symposium on Software Reliability Engineering. (ISSRE2015).
[9] The 25th IEEE International Symposium on Software Reliability Engineering.(ISSRE 2014).
[10] Accunetix Tool.
[11] OWASP Top 10 Attacks 2013: https://www.owasp.org/index.php/Top_10_2013whitepapers@contextis.co.uk
[13] Bin Wang, Lu Liu, Feng Li, Jianye Zhang, Tao Chen, Zhewan Zou, paper on "Research on Web Application Security Vulnerability Scanning Technology". IEEE, 2019.

[14] Stefano Russo, Marco Vieira, paper on "Security and Dependability of Cloud Systems and Services (Special Issue)" IEEE Transactions on Services Computing, 2017.
[15] 12th European Dependable Computing Conference.(EDCC2016).
[16] Abdul Razzaq, Ali Hur, Sidra Shabaz, Mudassar Masood, H Farooq Ahmad, "Critical analysis on Web Application Firewall", IEEE, 2013.
[17] Wu Qianqian, Liu Xiangjun Research and Design on "Web Application Vulnerability Scanning Service" IEEE 2014.
[18] Z.Ghanbari, Y. Rahmani, H. Ghaffarian, M. Hossein Ahmadzadegan "Comparative approach to web application firewall", IEEE, 2015.
[19] Sajjad Rafique, Mamoona Humayun, Bushra Hamid, Ansar Abbas, Muhammad Akthar, Kamil Iqbal "Web Application Security Vulnerabilities Detection", IEEE, 2015.
[20] IGN Mantra, Muhammad Alaydrus, HM Misni, "The web security and vulnerability analysis model on Indonesia Higher Education Institution", IEEE, 2016.