IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11677

Prometheus

Aditya Sachin Patil[1], Vaibhav Singh Rawat[2], Haresh Raju Kaneshan[3] ,Yashita Agarwal[4], Dr. Garima Sinha[5]

[1-5]Department of Computer Science and Engineering, FET- Jain University Bangalore, Karnataka, India

Abstract: Present Web Security is a serious concern. We learn with great regularity that websites, databases, and online services become inaccessible due to denial of service attacks or display modified information on the user or organization. In other high-profile incidents, millions of passwords, email addresses, and credit card information were leaked into the public, exposing users to both personal humiliation and financial risk. Web security is designed to avoid these kinds of attacks. Web Security is characterized more formally by the act of ensuring websites from unauthorized access, usage, alteration, destruction, or disruption. The higher the protection, the more trust users put on the application. Security plays a key role in achieving success for the application, especially in Web services. This essay will therefore discuss how users use cryptography today, the encryption concepts for databases, and the encryption concepts for the security of online service, thus understanding the issue of web system security.

Keywords: Protection,Cryptography,WebServices,Database

1. INTRODUCTION

The Web is now part of everyone's life and it constitutes the primary means of access to many useful services with strict security requirements. As a result, vulnerabilities on the web platform may enable vicious attacks with catastrophic consequences,ranging from economic losses.

Security-critical services are more and more supplied online today and this increases the need of effective defenses for the web platform. Today we are completely dependent on businesses or services that are totally digital or are supported by digital channels. Common things business leaders really think of, is a website really needed and how secure is our website to transact? With an increased amount of business across the digital landscape, we can see an upward trend of cyber attacks making the business websites vulnerable and leaving them at the mercy of the infiltrators, hence securing websites is important. Web security refers to protecting networks and computer systems from damage to or the theft of software, hardware, or data. It includes protecting computer systems from misdirecting or disrupting the services they are designed to provide. We need web security as recent studies conform a trend that has been observed in last 8 years: strong increase in (quality and number of) threats related to client-server / multi-tier applications, adopted in Web 2.0 applications,complex scenario, because preventions requires study of software components and of their interactions,critical components are always Web server and browser,other possible critical components: DBMS server and application server As it normally happens in computer science, when some kind of process is too error-prone, formal methods come to the rescue. In the last few years, many security researchers proposed to endow the web platform with more rigorous, analytical foundations. Their goal is designing models which allow for a precise reasoning on web security issues and developing effective tools to make the Web a safer place, relieving at least part of this burden from the shoulders of web developers and browser vendors. Given the complexity of the Web, however, research efforts in the area are quite scattered around many different topics and problems, and it is not easy to understand the import of formal methods on web security so far. One natural question is whether formal methods have been successful in this field or whether they can only be considered a theoretical exercise as of now: practical applications are important to showcase the effectiveness of formal methods at dealing with the problems mentioned above and encourage the web security community to synergise efforts with the formal methods community.

2. FEATURES

- **Malicious Files Scanner**

Antivirus Scanner that will scan your website for malicious files and will notify you if any are detected.

- **Normal Scan option**

The normal scan scans all files with the simple scan engine.

- **Deep Scan option**

The deep scan scans all files with the heaviest scan engine, but could show many false-positive threats.

- **Scan Customization**

You can choose which directories and files with specific extensions to be scanned. Files and directories can be

DOI: 10.17148/IJARCCE.2022.11677

whitelisted.

- **Customizable Scan Strings**

Additional scan strings can be added.

- **Detailed Information**

The script offers detailed information about the detected file like File Stats and Threat Information.

- **Security Check**

Powerful tool that will list all vulnerable PHP Functions that are enabled on your host.

- **Dashboard with File Stats**

On the Dashboard you can check the Statistics.

- **No database required**

The script works without database connection.

- **Optimized**

The script is very lightweight and won't overload your website.

- **Fully Responsive**

Accessible on many devices and screen resolutions like desktops , tablets as well as mobiles

3. METHODOLOGY

There are many risks associated with using Internet access for business activities. When you create a security policy, you need to balance the provision of services with the control of features and access to data. Computers connected to the network are more difficult to secure because the communication channels themselves are vulnerable.

As if it wasn't difficult enough to protect assets in the era of BYOD (Bring Your Own Device), corporate IT security is plagued and unknown heroes are surpassing more and more user access devices. You should consider the security of devices such as these printers. , Fax machines, and even routers and switches that make up the network. As if it wasn't difficult enough to protect assets in the era of Bring Your Own Device (), enterprise IT security-stricken heroes have gone beyond more and more user-access devices to printers. You should consider the security of your device, such as. Fax machines, even routers and switches.

The concept of layered defense is a bit outdated. However, enterprise networks are becoming more complex and the nature of the threat is evolving. Therefore, in today's threat context, layered defenses are still the best way to protect your application.And some of them would be :-

Known Signatured-based scans:

Scanning for vulnerabilities is one of the easiest ways to predict the potential for a hacker to break into your system. This is the process of identifying security weaknesses and bugs in the system and the software running on it. This is an integral part of web security and keeps your organization up-to-date with attack vectors.

Suggest Best practices for configuration:

Best practices are important in processes that need to function properly. They are simply the best way to do things, solved by trial and error, and proven to be the wisest course of action, and are the foundation of web security.

Provide useful stats and stack trace:

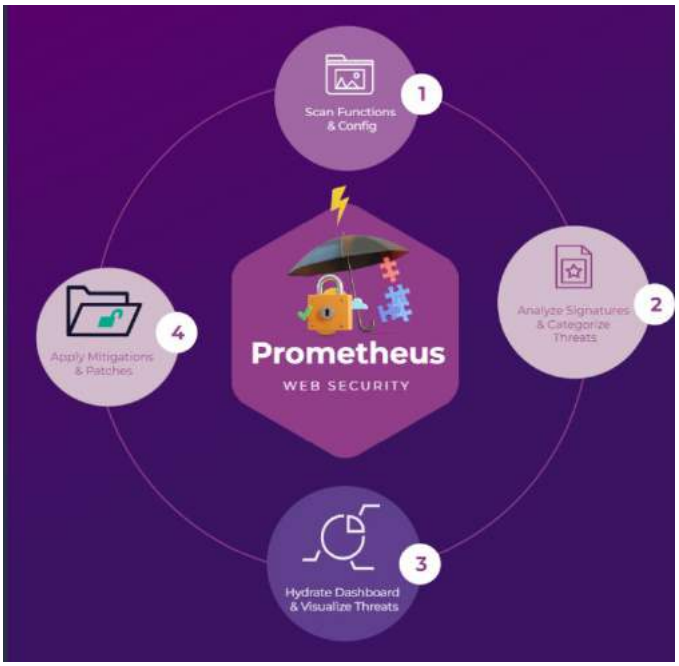
Statistics are an integral part of site analysis for performance and reliability. Incident stack traces are needed to identify the root cause of the problem and assist in debugging the code base..

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

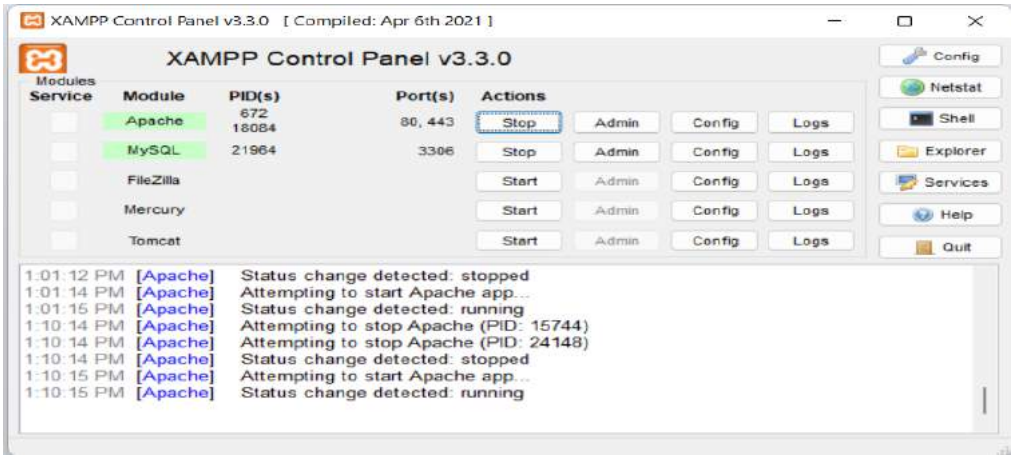
DOI: 10.17148/IJARCCE.2022.11677



Easy to setup & use for non-technical users:
The tool is easy to set up without any technical knowledge and provides an intuitive approach that is easy for the average user to use..

4. RESULTS

XAMPP controller is used to initialize the Apache Http server and MySQL for the dummy website to test for vulnerabilities.



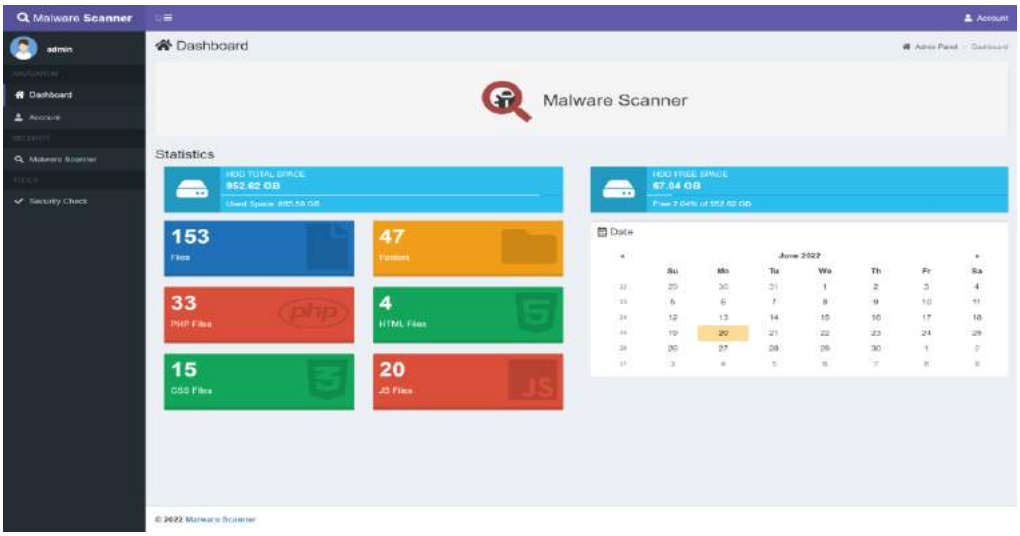
Use case : localhost:3000/"program_name"/scanner, on the url box of any web browser.
Here our program name is dummy..

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

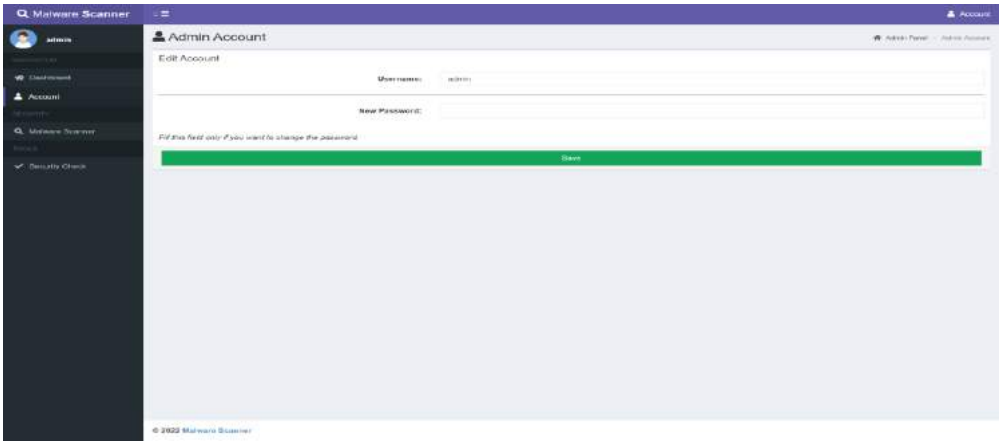
International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

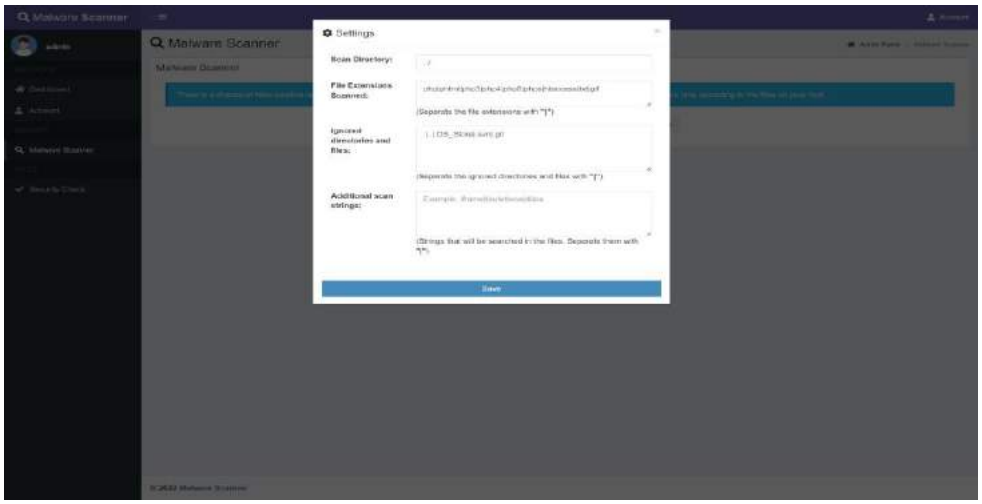
DOI: 10.17148/IJARCCE.2022.11677



This is the main Dashboard where all the statistics are mentioned, like the storage space left on the drive, the number of php files, html files, folders and so on. We can also navigate to the account and malware scanner tabs from here



This is the Account tab, where one can change the account name and details



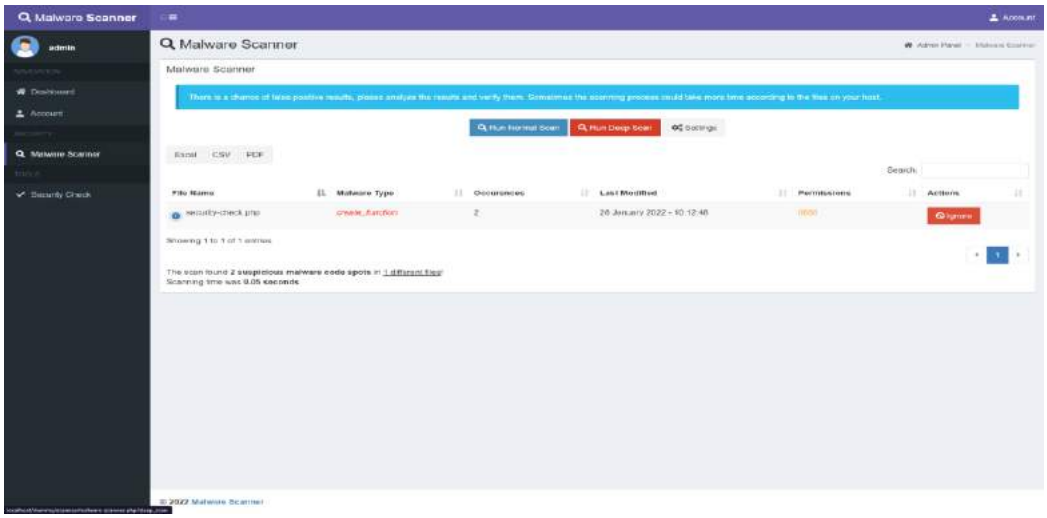
These are all the options in the settings tab, where we can change directory scope, the file extension types, the directory or files which need to be ignored and if any additional strings need to be added.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

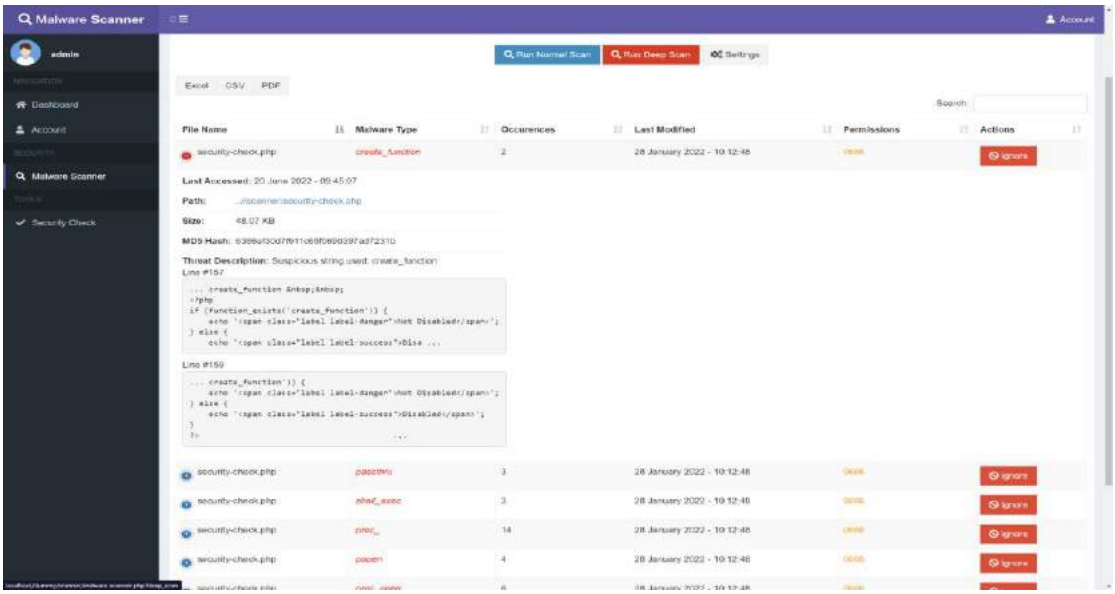
International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

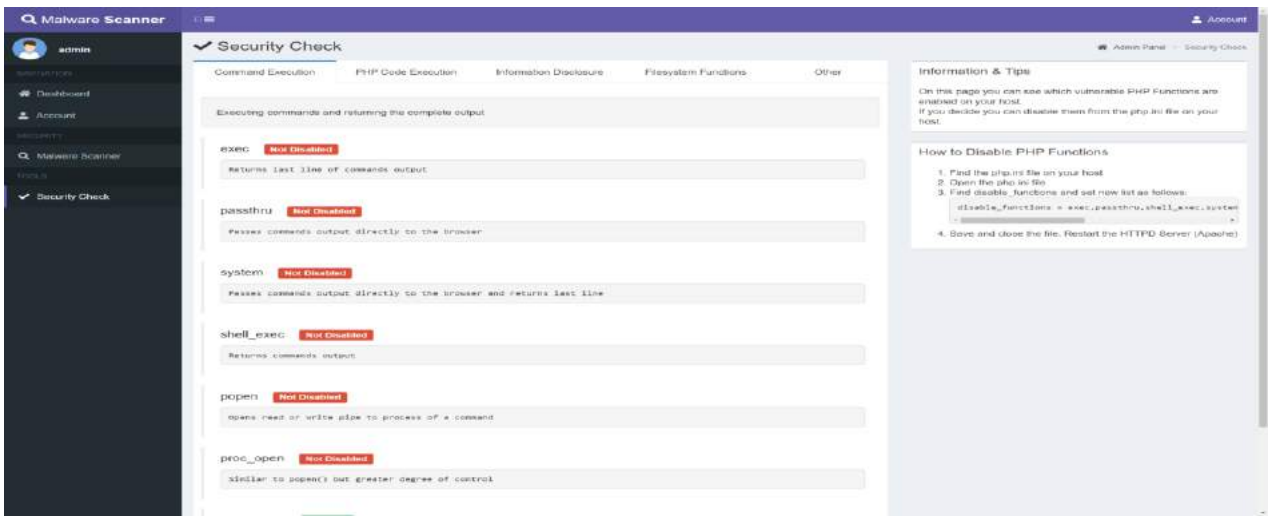
DOI: 10.17148/IJARCCE.2022.11677



This is the normal scan results where it only found 1 malware on the specified folder



These are the detailed results of the deep scan, it found 6 vulnerabilities in our dummy website



International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.11677

For a more detailed result, the security check tab displays all the functions which are vulnerable in the specified folder grouped by its threat type like command execution and others.

5. CONCLUSIONS AND FUTURE SCOPE

Web application security consists of a large number of attack areas and defenses. Protecting your web application with just one technique, or just one layer of the stack, is not enough. Vulnerabilities in platforms or protocols such as TCP and HTTP can have a devastating impact on application security and availability, as well as attacks on the application itself. A complete stack of mitigation solutions is required to achieve an aggressive security regime for web applications. It is important to note that a comprehensive approach requires collaboration between network, security, operations, and development teams. Each team is responsible for protecting the application and its important data. Organizations are under pressure to respond quickly to dynamically increasing cybersecurity threats. Attackers use the attack lifecycle, forcing organizations to develop vulnerability management lifecycles as well. The vulnerability management lifecycle is designed to counter attackers' efforts as quickly and effectively as possible. This project described the vulnerability management lifecycle in terms of vulnerability management strategies. You have gone through the steps of asset inventory creation, information flow management, risk assessment, vulnerability assessment, reporting, and remediation.This project scripts can be in as a add-on for a website template/boilerplate to provide a better secure initial config

REFERENCES

[1.] Silva, Nimesh. (2020). Threats to Web Security. 10.13140/RG.2.2.29526.27201.
[2.] Sharma, Sachin Kumar, Arjun Singh, Punit Gupta and Vijay Kumar Sharma. “Web Security Vulnerabilities.” Cybersecurity (2021): n. pag.
[3.] Bugliesi, Michele, Stefano Calzavara and Riccardo Focardi. “Formal methods for web security.” J. Log. Algebraic Methods Program. 87 (2017): 110-126.
[4.] Bozic, Josip, Bernhard Garn, Ioannis Kapsalis, Dimitris E. Simos, Severin Winkler and Franz Wotawa. “Attack Pattern-Based Combinatorial Testing with Constraints for Web Security Testing.” 2015 IEEE International Conference on Software Quality, Reliability and Security (2015): 207-212.
[5.] Fonseca, José, Marco Paulo, Amorim Vieira and H. Madeira. “Evaluation of Web Security Mechanisms Using Vulnerability & Attack Injection.” IEEE Transactions on Dependable and Secure Computing 11 (2014): 440-453.
[6.] Dwivedi, Ashish Kumar and Santanu Kumar Rath. “Formalization of web security patterns.” INFOCOMP Journal of Computer Science 14 (2015): 14-25.
[7.] Qian, Li, Jiahua Wan, Lu Chen and Xiuming Chen. “Complete Web Security Testing Methods and Recommendations.” 2013 International Conference on Computer Sciences and Applications (2013): 86-89.
[8.] Foss, J. and Nina Ingvaldsen. “Web Application Security.” Cybersecurity Blue Team Toolkit (2019): n. pag.