Scanning Websites for Vulnerabilities: Ultimate Guide

BY MORGAN DUBIE

WordPress Security

Introduction

Regularly scanning websites for vulnerabilities is one of the most critical steps for website owners to take regarding security. Not only does it help prevent unauthorized access, but it can also improve the overall user experience.

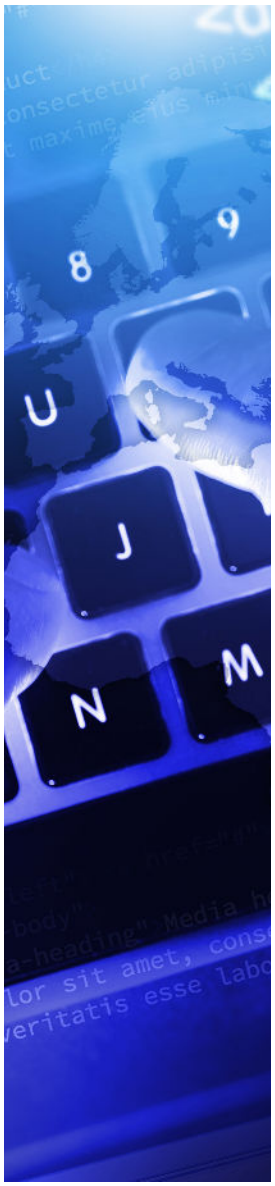
In this blog post, I'll discuss everything you need to know about scanning websites for vulnerabilities. You'll learn how vulnerability scanning can help you identify and prevent security breaches and the benefits of website vulnerability scanning.

Introduction

What you'll learn:

- What is website vulnerability scanning?
- How do vulnerability scanners work?
- Why is scanning for vulnerabilities important?
- Features of the best web application vulnerability scanners
- Different types of scans
- Common website vulnerabilities
- The process of scanning websites for vulnerabilities

SCANNING WEBSITES FOR **VULNERABILITIES 2023**



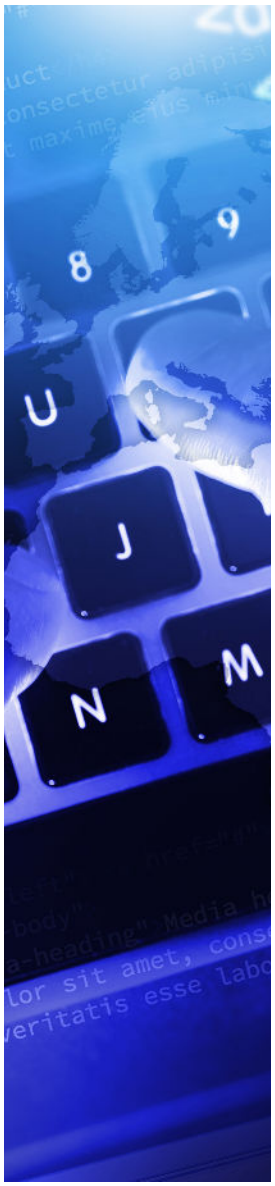
What is website vulnerability scanning?

One of the most common ways to check a website against a massive list of known security vulnerabilities is website vulnerability scanning. Security experts usually scan a website to identify security flaws in a web application or website as part of a larger vulnerability assessment.

How do vulnerability scanners work?

Vulnerability scanning systematically tests a website or web application for potential security weaknesses and vulnerabilities.
Using a vulnerability scanner is vital for website security. Firstly, it performs manual or automated scans, preventing data breaches and system downtime.

SCANNING WEBSITES FOR **VULNERABILITIES 2023**



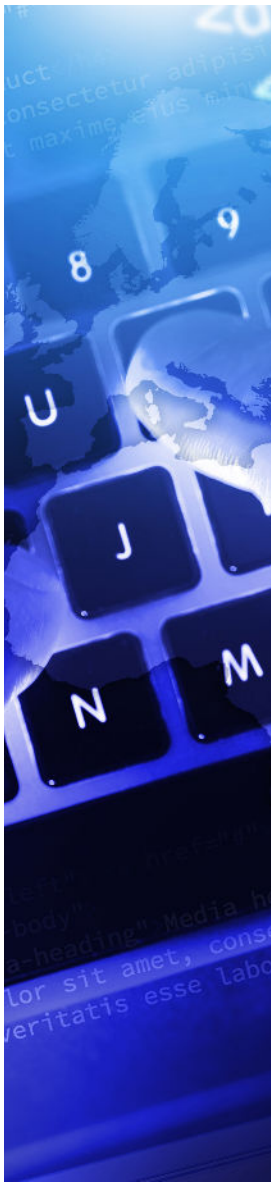
How do vulnerability scanners work? (cont'd)

Secondly, it proactively identifies and addresses security weaknesses, reducing potential incidents. Ultimately, vulnerability scanners are wildly important and beneficial!

Why is scanning websites for vulnerabilities important?

Having a vulnerability scanner is for sure a website security best practice! It's crucial for maintaining your website's security. Here's a list of reasons why scanning for vulnerabilities is important:

SCANNING WEBSITES FOR **VULNERABILITIES 2023**



Why is scanning websites for vulnerabilities important? (cont'd)

- **Identifies security weaknesses**

Vulnerability scanning helps identify security weaknesses in web applications or websites, which allows you to take corrective action before something terrible happens.

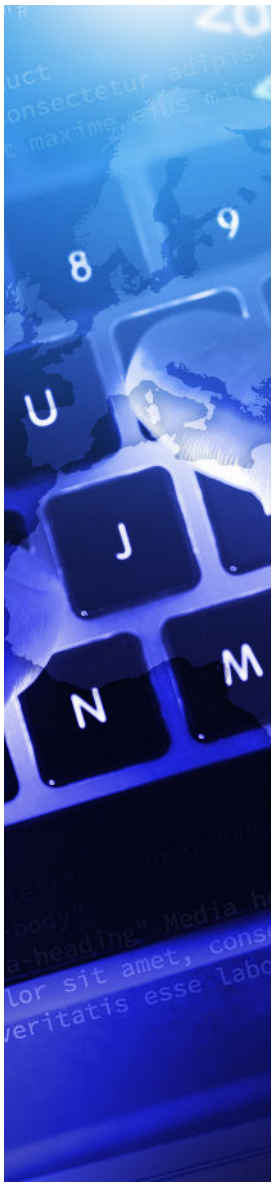
- **Helps stay compliant**

Many industries require compliance with specific security standards, and vulnerability scanning can help ensure that you meet these requirements.

- **Improves overall security posture**

By identifying and addressing vulnerabilities, vulnerability scanning can help improve the overall security posture of your organization. This is super important regarding how your business earns and maintains customers' trust, right? No one wants to do business with an insecure company. Period.

SCANNING WEBSITES FOR **VULNERABILITIES 2023**



Why is scanning websites for vulnerabilities important? (cont'd)

- **Reduces risk of data breaches**

Vulnerability scanning helps identify and address security weaknesses that can lead to data breaches, reducing the risk of exposing sensitive data. Nobody wants that to happen!

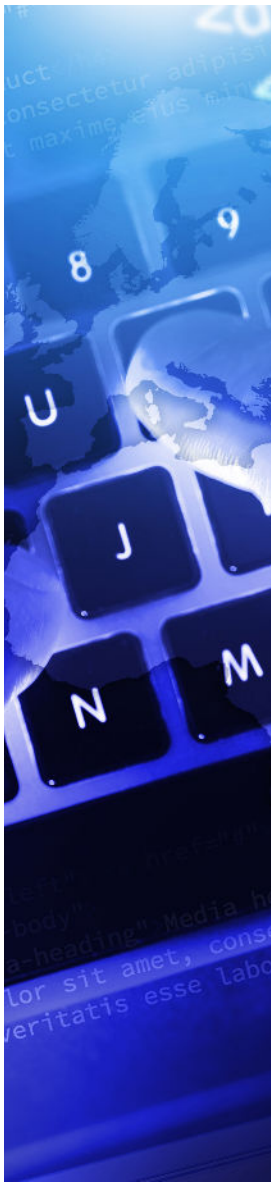
- **Saves time and money**

Addressing security issues proactively can save you time and money in the long run, as it reduces the likelihood of costly security incidents. And everyone likes the idea of saving money, am I right?

- **Builds customer trust**

As I previously mentioned, customers are more likely to trust organizations that take their security seriously, and vulnerability scanning is a key part of a comprehensive security strategy.

SCANNING WEBSITES FOR **VULNERABILITIES 2023**



Features of the best web application vulnerability scanners

Website vulnerability scanners are crucial tools businesses, and website owners utilize to ensure the security of their websites. They aid in identifying potential vulnerabilities that hackers and cybercriminals could exploit.

However, the effectiveness of website vulnerability scanners depends on their key features. Therefore, the best website vulnerability scanners possess several key features that enable them to identify vulnerabilities and protect online assets.

Some of these top features include:

SCANNING WEBSITES FOR **VULNERABILITIES 2023**

1. Comprehensive scanning

The scanner should be able to scan the entire website, including all pages, files, and forms, to identify potential vulnerabilities. This ensures that all website areas are thoroughly checked for potential security issues.

2. Real-time monitoring

Scanners should be able to monitor the website in real-time, alerting the website owner to any potential threats as soon as they are detected. This allows for quick and effective remediation of vulnerabilities before they can be exploited.

"Vulnerability scanning systematically tests a website or web application for potential security weaknesses and vulnerabilities."

- MORGAN

SCANNING WEBSITES FOR **VULNERABILITIES 2023**

3. Customizable scans

The scanner should allow for the customization of scans, including the ability to specify which pages or areas of the website to scan. This allows for more targeted scans, saving time and resources while effectively identifying vulnerabilities.

4. Remediation guidance

Vulnerability scanners should provide guidance for remediating any vulnerabilities detected, including detailed instructions and resources to assist website owners in addressing potential security issues.

"Vulnerability scanning systematically tests a website or web application for potential security weaknesses and vulnerabilities."

- MORGAN

SCANNING WEBSITES FOR **VULNERABILITIES 2023**

5. Reporting

Comprehensive reports detailing the vulnerabilities detected, their severity and recommended remediation steps. This information is critical for website owners to prioritize their efforts and ensure their website is secure.

6 Integration

Lastly, scanners should be able to integrate with other security tools and platforms, such as firewalls and intrusion detection systems, to provide a more comprehensive security solution for the website.

"Vulnerability scanning systematically tests a website or web application for potential security weaknesses and vulnerabilities."

- MORGAN

Different Types of Scans

We're covering a ton of ground in this article! Let's go even further and discuss the different types of scans available.

Active and Passive Vulnerability Scans

Active and passive website vulnerability scanning are two approaches to identifying and detecting website vulnerabilities.

Passive Scanning:

Involves monitoring and collecting information from a website without actively sending any requests or inputs to the website.

Passive scanning can be done by analyzing traffic logs, network traffic, or other data sources. Passive scanning is a non-intrusive approach that can identify information leaks, unencrypted data transmissions, and other vulnerabilities that may be visible from the network traffic.

DID YOU KNOW?

- The cost of cybercrime is predicted to hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025.
- One way that hackers take advantage of code vulnerabilities and open-source flaws is via zero-day exploits. Recently a ransomware gang used a new zero-day flaw to steal data on 1 million hospital patients

Different Types of Scans (cont'd)

Active Scanning:

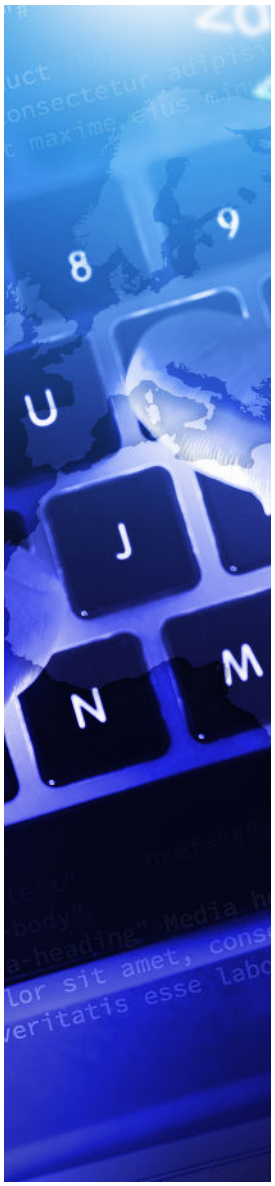
Sending requests and inputs to a website to see how it responds. Active scanning is an intrusive approach that simulates an attacker's behavior and can identify vulnerabilities such as SQL injection, cross-site scripting (XSS), and other security weaknesses.

Active scanning can be performed using various tools and techniques, such as vulnerability scanners, penetration testing, or automated scripts.

They help readers jump to topics of interest

- The cost of cybercrime is predicted to hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025.
- One way that hackers take advantage of code vulnerabilities and open-source flaws is via zero-day exploits. Recently a ransomware gang used a new zero-day flaw to steal data on 1 million hospital patients

SCANNING WEBSITES FOR **VULNERABILITIES 2023**



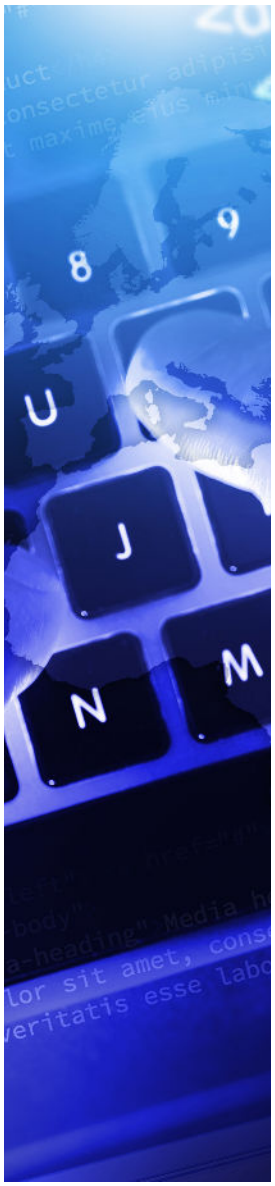
Authenticated and Unauthenticated Scans

Web application vulnerability scans can also be classified depending on whether or not you're performing the scan with administrator privileges or credentials. This is called authenticated vs. unauthenticated scans.

Authenticated Scanning:

Testing the web application with valid login credentials, allowing the scanner to access deeper functionality and test for more complex vulnerabilities. This type of scan simulates the behavior of a trusted user with access to sensitive data or functionality. Authenticated scans can identify vulnerabilities such as privilege escalation, session hijacking, and other security issues that require authenticated access.

SCANNING WEBSITES FOR **VULNERABILITIES 2023**



Unauthenticated Scanning

Testing the web application without prior authentication or login credentials. This type of scan simulates the behavior of an external attacker attempting to exploit vulnerabilities in the web application. Unauthenticated scans can identify vulnerabilities such as SQL injection, cross-site scripting (XSS), and other security weaknesses accessible without authentication.

Other Types of Scans:

Here's a brief look at some of the other types of vulnerability scans you can perform:

Black Box Scanning

This type of scan involves testing a web application without any prior knowledge of its internal workings, such as its source code. The scanner will typically simulate different types of attacks and record any vulnerabilities it detects.

White Box Scanning

In contrast to black box scanning, white box scanning involves testing a web application with access to its internal workings, such as its source code or architectural design. This can help identify more complex vulnerabilities that are not easily detected through black box scanning.

Static Application Security Testing (SAST)

SAST is a type of white box scanning that involves analyzing the source code of an application for security vulnerabilities. It can identify potential vulnerabilities early in the development cycle and help developers fix them before the application is released.

Other Types of Scans:

Here's a brief look at some of the other types of vulnerability scans you can perform:

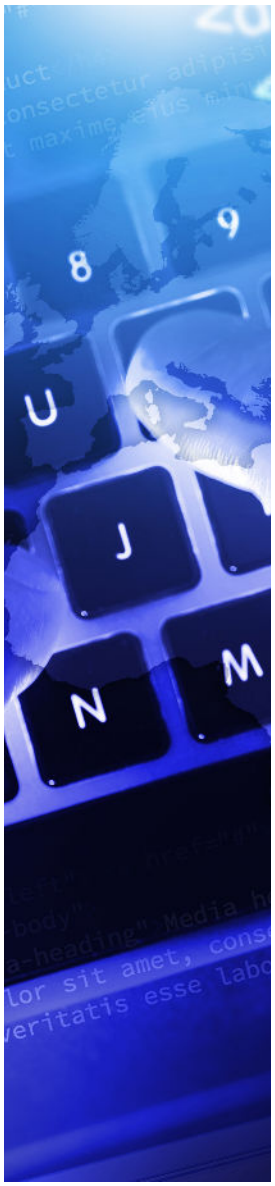
Dynamic Application Security Testing (DAST)

DAST is a type of black box scanning that involves testing a live application for vulnerabilities. This can help identify vulnerabilities that may not be apparent in the source code, such as misconfigured servers or authentication issues.

Interactive Application Security Testing (IAST)

IAST is a type of white box scanning combining SAST and DAST elements. It involves analyzing the application's source code and testing it in a live environment for vulnerabilities. This approach provides more comprehensive testing than either SAST or DAST alone.

SCANNING WEBSITES FOR **VULNERABILITIES 2023**

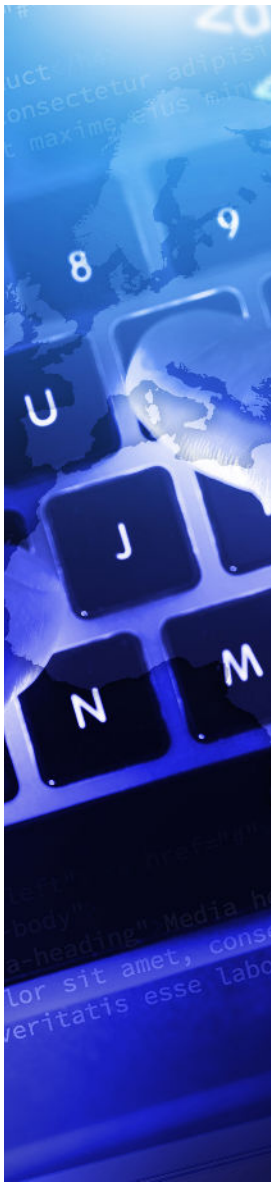


Common Website Vulnerabilities

Website vulnerabilities are weaknesses or flaws in a website's code, configuration, or architecture that attackers can exploit to gain unauthorized access, steal data, or disrupt the website's operations. Various factors, such as poor coding practices, misconfigured servers, outdated software, or weak passwords, can cause these vulnerabilities.

Here are some of the most common website vulnerabilities we're faced with today:

SCANNING WEBSITES FOR **VULNERABILITIES 2023**



Common Website Vulnerabilities (cont'd)

- **SQL Injection**

This vulnerability allows attackers to inject malicious SQL code into a website's database, potentially allowing them to access sensitive data or execute unauthorized commands.

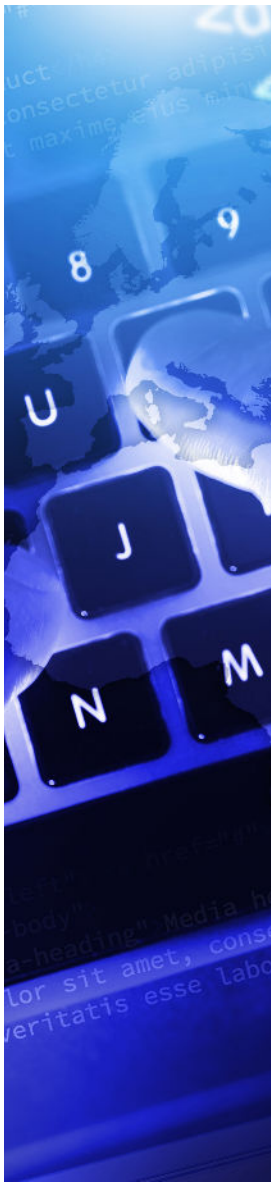
- **Cross-Site Scripting**

Many industries require compliance with specific security standards, and vulnerability scanning can help ensure that you meet these requirements.

- **Cross-Site Request Forgery**

This vulnerability allows attackers to trick users into executing unauthorized actions on a website, such as changing their password or making unauthorized purchases.

SCANNING WEBSITES FOR **VULNERABILITIES 2023**



Common Website Vulnerabilities (cont'd)

- **Broken Authentication and Session Management**

Attackers bypass authentication mechanisms or hijack user sessions, potentially giving them unauthorized access to the website's resources.

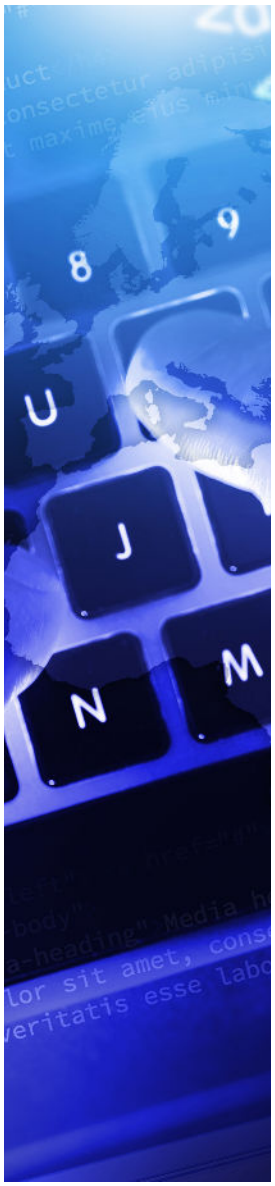
- **File Inclusion Vulnerabilities**

Allows attackers to include and execute arbitrary files on a website's server, potentially allowing them to access sensitive data or execute unauthorized commands.

- **Server Misconfigurations**

This vulnerability includes issues such as weak passwords, open ports, and unsecured services on the website's server, potentially allowing attackers to gain unauthorized access or disrupt the website's operations.

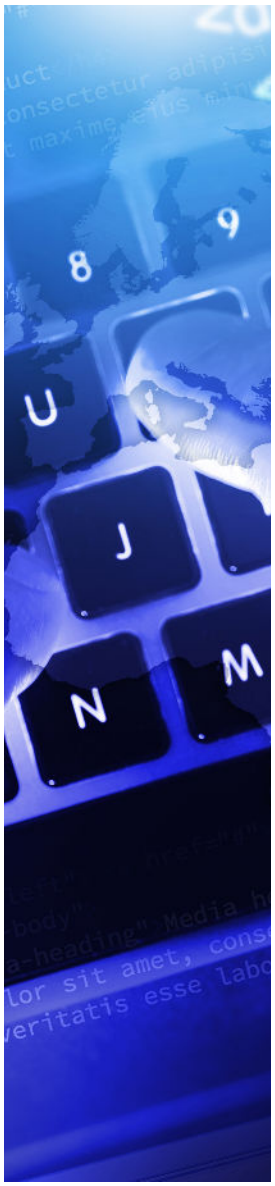
SCANNING WEBSITES FOR **VULNERABILITIES 2023**



Process of Scanning Websites for Vulnerabilities

The website vulnerability scanning process should be systematic, repeatable, and well-documented to ensure all vulnerabilities are properly identified, assessed, and remediated. Keeping the scan results and reports confidential and secure is also important to avoid disclosing sensitive information to unauthorized parties.

SCANNING WEBSITES FOR **VULNERABILITIES 2023**



Let's take a look at the typical process of website vulnerability scanning:

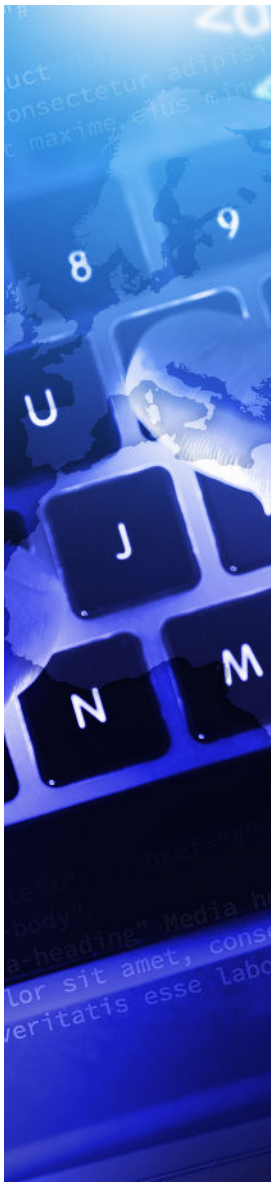
- **Analysis**

The scanner then analyzes each page and resource of the website, looking for vulnerabilities such as SQL injection, cross-site scripting, file inclusion, and other security weaknesses. This can be done using various techniques such as code analysis, payload injection, and pattern matching.

- **Exploitation**

Once the scanner identifies a vulnerability, it may attempt to exploit it by sending specially crafted requests or payloads to the target website, simulating the behavior of an attacker. This can be done using various techniques such as SQL injection, cross-site scripting, and command injection.

SCANNING WEBSITES FOR **VULNERABILITIES 2023**



Scanning Process (Cont'd)

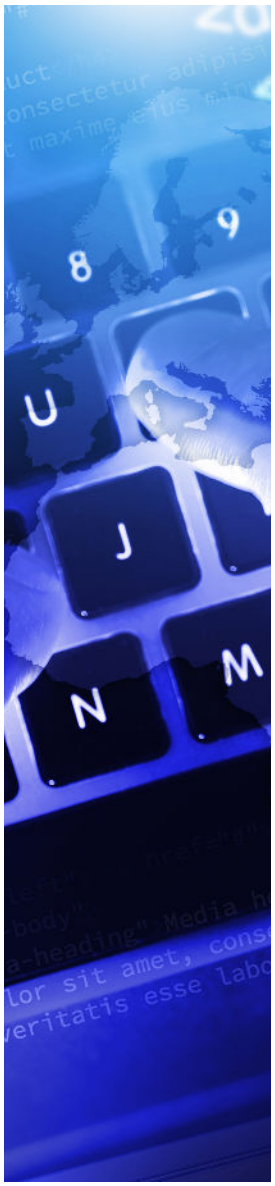
- **Reporting**

Next, the scanner reports the scan findings, including a summary of the vulnerabilities identified, their severity and impact, and recommended remediation steps. The report may include additional information, such as the vulnerability details, the proof-of-concept exploits used, and the steps to reproduce the issue.

- **Remediation**

Based on the scan results, the website owners and developers can remediate the identified vulnerabilities, including patching the affected systems, updating the software and configurations, and implementing security controls and best practices.

SCANNING WEBSITES FOR **VULNERABILITIES 2023**



Summary

Scanning websites for vulnerabilities is essential to protecting your website from harm. In this ultimate guide on scanning websites, we reviewed everything from what a website vulnerability scanner is to the scanners' steps when scanning your website. We also looked at some of the different types of website vulnerability scans and the features to look for when choosing a scanner.

I hope this guide has been helpful to you! As usual, please never hesitate to contact me with any questions or concerns!

Key Takeaways

What we've learned:

- What scanning websites for vulnerabilities is and why it's important
- Features of the best web application vulnerability scanners
- Different types of scans
- Common website vulnerabilities
- How the scanners work/the process of the scans

Have Questions?

(802) 734 - 4252

I'm always available to answer any questions you may have. Call or email me today, I would love to hear from you!