



LEARN TO IMPROVE

# WEBSITE SECURITY

*Step-by-Step Guide for Secure Website*



# Table of Contents

This workbook is designed to help you with tips and strategies on how to increase your website speed.

<b>Introduction</b>	<b>01</b>
<b>Types of Security Attacks</b>	<b>03</b>
<b>How to Perform a Website Security Audit?</b>	<b>04</b>
• <b>Step 1: Scanning for Vulnerabilities</b>	<b>06</b>
• <b>Step 2: Exploitation of Vulnerabilities</b>	<b>11</b>
<b>Conclusion</b>	<b>15</b>

# Introduction To Website Security

A website security audit scans your website and its server for existing or potential weaknesses that hackers can exploit.

It covers your website's entire infrastructure, from its core software to extensions, themes, server settings, SSL connection, configurations, etc.

Once all loopholes and gaps have been identified, the next step is to conduct penetration tests or pentests. Under this, security teams launch pseudo hacking attacks against your application, mimicking ones that happen in real life. The vulnerabilities detected in the first step are targeted in order to assess the risk associated with them.



The purpose of website security audits is to proactively look for discrepancies in your website's architecture, and eliminate them before hackers with malicious intent can notice.

Industry experts always press on the importance of regular security auditing, as hackers will constantly challenge your website's

safety using every trick in the toolbox.

Simply following basic practices and leaving everything else to fate is not the answer. Admins have to constantly be on their toes and perform rigorous scanning and testing so that there is little to no scope of exploitation.

# Types of **Security Attacks**

- Financial frauds
- Phishing
- Cross-Site Scripting (XSS)
- Man in the middle
- DDoS Attacks
- Brute Force Attacks
- SQL Injections


# How To Perform A Website Security Audit?




For security audits, you will have to use online tools or hire professional services. There are many free and paid tools and services available online for security scanning.

As explained above, website security audits are divided into two steps. So let's discuss these steps a bit more in detail and look at the tools you can use.

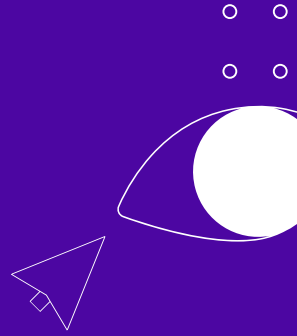
- **STEP 1: SCANNING FOR VULNERABILITIES**
- **STEP 2: EXPLOITATION OF VULNERABILITIES**



**29% of your website traffic has malicious intentions and wish to attack you. 92.4% malware delivery takes place through emails on given email addresses on your website.**



# Scanning For Vulnerabilities



In this first step, the tool you choose will go through all aspects of your website's security. It will screen your database, directories, files, themes, plugins, web server, etc to detect vulnerabilities, malware, viruses, and lax security measures.

Here is a list of tools you can use:

- Sucuri Sitecheck
- Qualys SSL Server Test
- Intruder

There are three more tools I would like to suggest, just in case you want alternatives:

- Web Cookies Scanner
- SiteGuarding
- Observatory



# Sucuri Sitecheck

## Free website security check & malware scanner

Enter a URL like example.com and the Sucuri SiteCheck scanner will check the website for known malware, viruses, blacklisting status, website errors, out-of-date software, and malicious code.

Sucuri's SiteCheck is free scanning tool that will check:

- Website source code for malware, viruses, malicious code, and infected file locations.
- Check if your website has been blacklisted by website security authorities like PhisTank, Google, etc.
- Find out if all website components are up-to-date i.e., CMS version, plugins, or extensions.

- It will also see if there are any configuration or other security issues present.

Based on its scan, Sucuri reveals the types of threats each loophole is vulnerable to and gives hardening recommendations. It is a pretty slick tool if you want to ensure that you're not missing out on any security best practices.

# Qualys SSL Server Test



Qualys SSL server test scans your SSL/TLS server connection and checks for any misconfigurations or vulnerabilities. It grades your website on this basis and shows you the level of protocol support, cipher strength, key exchange, etc.

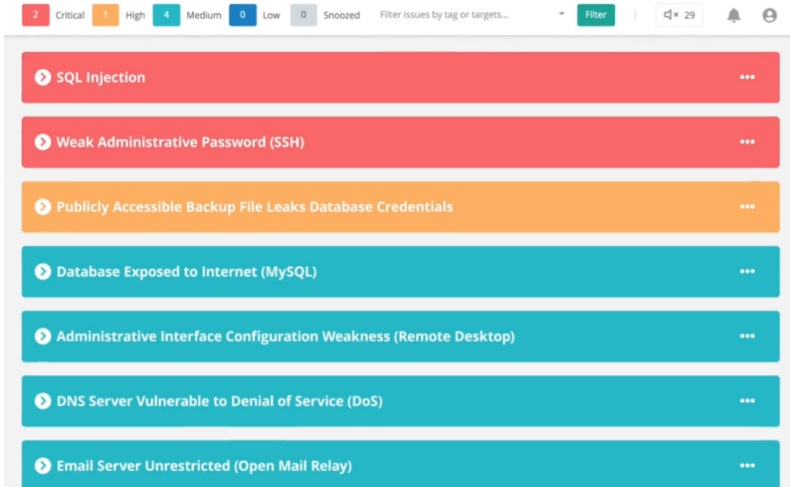
It is a free tool, and all you have to do is add your Hostname and click submit to get a report.

If you want to ensure your website is following standard communication protocol and encryption, then this tool will definitely help you out.

# Best Security Practices



# Intruder



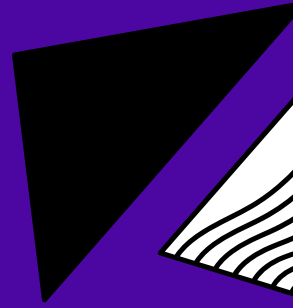
Intruder is an enterprise-level, cloud-based vulnerability scanner. It checks your entire web application for bugs, configuration weaknesses, and missing patches. Your website CMS will also be scanned for common security issues.

Intruder prioritizes issues by assessing the risk associated with them, so that you can patch critical loopholes first, and then move on to the less serious ones.

It also suggests easy to understand remedial measures for each threat, and proactively monitors your systems.

Moreover, you can integrate it with applications like Slack or Jira and get notified about the latest threats in your site instantly through messages.

# Exploitation Of Vulnerabilities



Now that you have sufficient knowledge of your website's security status and the issues it harbors, it is time to deploy Pentest (penetration testing) tools and judge the severity of each vulnerability. F

or this as well, you can use the following tools to run autonomous scans:

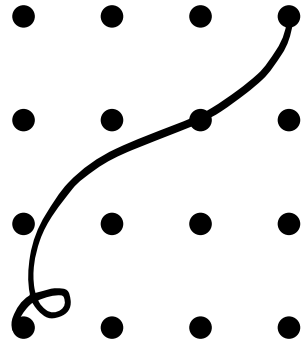
Tools explained are:

- Website Vulnerability Scanner By Pentest-tools
- W3AF
- Metasploit

Some alternatives:

- nmap
- John the ripper
- Kali Linux

# Website Vulnerability Scanner By **Pentest-tools**



This website vulnerability scanner is an extensive package covering a wide range of threats and security issues.

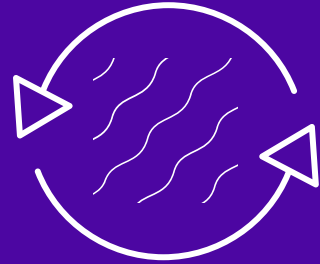
You could say that it is an end-to-end website security audit solution, as it gathers security information and conducts application testing, CMS testing, infrastructure testing, and SSL testing.

The company offers two solutions:

- Light Scan
- Full scan

In the light scan, 20 HTTP requests are sent to the server, whereas the Full scan sends up to 10,000 HTTPS requests and conducts thorough testing.

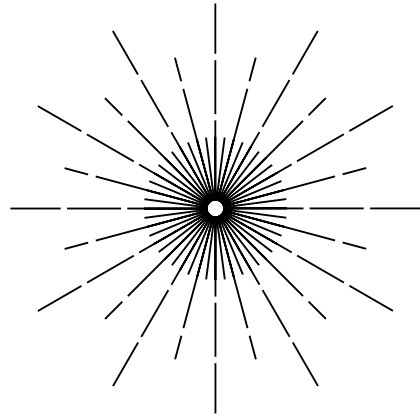
# W3AF



w3af is a web application attack and audit framework. You can use it to identify more than 200 vulnerabilities like SQL injection, cross-site scripting, guessable credentials, unhandled application errors, DNS spoofing, and PHP misconfigurations.

It is an open-source tool that performs pentests using techniques like payload injection into various kinds of HTTP requests, integrating web and proxy servers into the code, sending fast HTTP requests, etc.

# Metasploit



Metasploit is an indispensable penetration testing tool used by most web security pros.

Operating Metasploit is easy, you just have to point it towards your target website, pick an exploit, choose which payload to drop, and launch your attack. It has an extensive database that records all kinds of exploits.

Once you've identified all your weaknesses, you can launch attacks through this tool and determine your store's risk profile.

Metasploit is the most used pentest framework thanks to the elaborate functionality it offers. It has a command-line interface and automates most pentestive tasks that were previously laborious. It has both open source and paid services.

More and more features get added to Metasploit every year, so if you want to conduct a website security audit for your website, then this tool comes highly recommended and is a must-use!



# Finally...

A website security audit is a great way to stay at the top of your website's security status and ensure that you put in your best efforts, and minimize infiltration threats.

The best part is that there are a lot of free scanning tools you can find online, empowering website owners the ability to perform audits autonomously with little help from third parties.

Get fully-managed hosting that takes care of speed, security, monitoring with Webscoot.io.

Run on AWS for fixed cost >>





**SCAN THIS QR CODE FOR MORE  
EBOOKS ON ECOMMERCE**

