



NEGATIVE PID

WHITE PAPER

ENHANCING WORDPRESS SECURITY

- ▶ **A COMPREHENSIVE APPROACH TO VULNERABILITY CHECKS WITH R AND LINUX**

December 2023



@2023 Negative PID

<https://negativepid.com>

Contents

- I. INTRODUCTION
- II. UNDERSTANDING WORDPRESS VULNERABILITIES
- III. UNDERSTANDING THE IMPACT OF A DATA LEAK OR A HACKING ATTACK
- IV. VULNERABILITY ASSESSMENT METHODOLOGIES
- V. RATIONALE FOR AUTOMATING VULNERABILITY CHECKS IN WORDPRESS
- VI. BUILDING AN AUTOMATED VULNERABILITY TESTING FRAMEWORK IN R
- VII. CASE STUDIES AND USE CASES
- VIII. BEST PRACTICES FOR WORDPRESS SECURITY
- IX. CONCLUSION

I. Introduction

According to W3Techs Web Technology Surveys, WordPress powers **42.8%** of all websites on the Internet and holds **62.7%** of the known CMS (Content Management Systems) market share globally.

Among the most popular websites using WordPress we find Microsoft.com, Vimeo.com, Mozilla.org, Zoom.us, and Digidigit.org. WordPress official statistics indicate that this translates into monthly volumes of 409 million unique visitors, 20 billion page views, 70 million new posts and 77 million new comments.

WORDPRESS MONTHLY VOLUMES

20 Billion

Page views

70 Million

New Posts

77 Million

New comments

With numbers as such, WordPress holds a steady position ahead of website technology titans like Shopify, Joomla, Squarespace, and Wix. The secret to its success lays in its simplicity of use, its wide ecosystem of integrations, and its flexibility. Expert professionals and newbies alike can use WordPress to create content and publish it on the web, taking advantage of its complete framework for any commercial and personal purpose.

WordPress daily handles complex tasks such as credit card payments, and stores sensitive information on business and their customers.



Being so popular, WordPress offers a wider and wider surface to attacks. According to JetPack, a popular WordPress plugin set, there are 30,000 websites hacked each day on a global scale. With a simple calculation, it's plausible to infer that **10-12,000 WordPress sites are hacked daily.**

It then becomes obvious why maintaining the security of WordPress websites is of paramount importance to each website owner.

Even if the website doesn't process any payments or handles financial information, it still holds valuable information that can be exploited in several ways. This includes **account credentials, confidential information about the business, the technology in use** by the company, the **names of upper management and key employees, company assets** and plans.

The purpose of this white paper is to educate about risk mitigation and the importance of adopting security routines to keep your assets safe and protected, so that you can ensure your customers' and users' safety while browsing and using your website.

Particular importance is given to minimizing the risk of revenue loss due to data leaks, direct attacks, and reputation damages that come with hacking incidents.

We will also show you how we solved known issues and challenges with a data-driven approach and automation for our services.



II. Understanding WordPress vulnerabilities

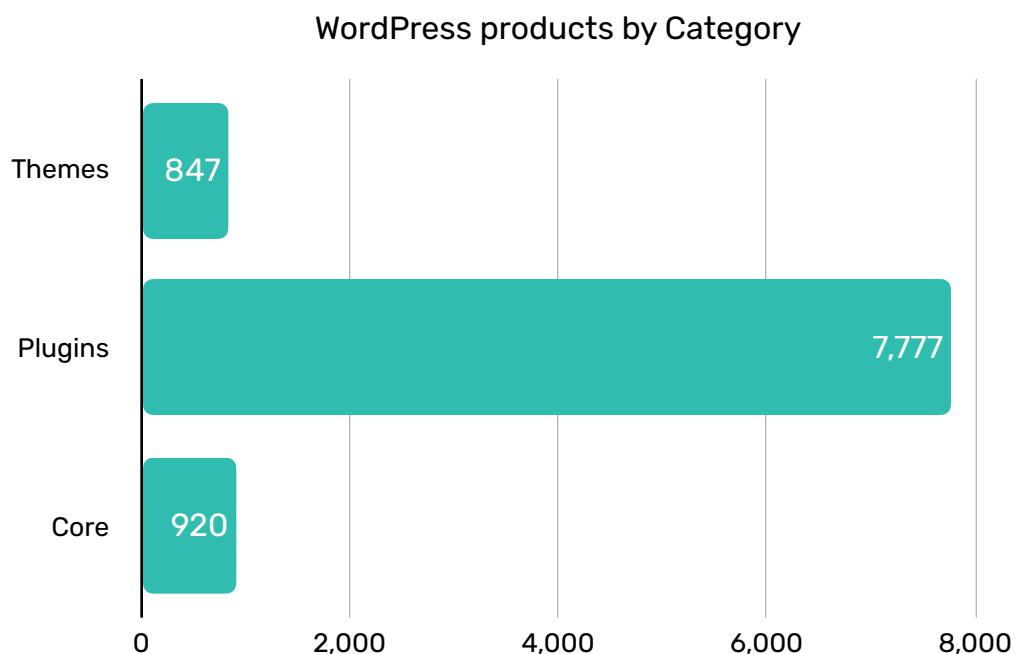
WordPress assets are canonically classified into three buckets:

- ▶ Core
- ▶ Plugins
- ▶ Themes

Core assets are WordPress components that carry general information on the WordPress version and configuration. These also include server components outlining the underlying technology for the WordPress website.

WordPress plugins allow for external service integration, such as database tables and queries, API integrations, and other functions.

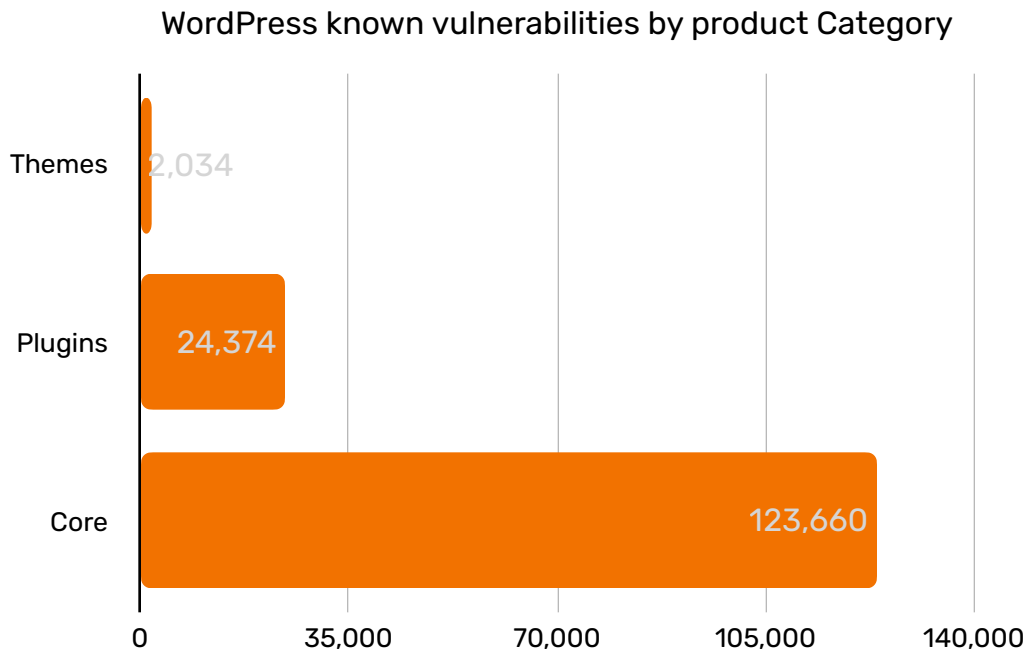
Finally, WordPress themes are skins that can be applied to the WordPress website to change its look and functionality, including CSS, templates, and customization settings.



Each category includes hundreds (if not thousands) of products. And each product category has specific vulnerabilities. These change every day as new threats are discovered, validated, and classified, or old threats are resolved and archived.

However, **the number of vulnerabilities related to each category is not directly proportional to the number of products or components.**

Indeed, the vast majority of the vulnerabilities affects Core products and is largely due to misconfigurations or lack of configuration (i.e., installing WordPress without changing its standard settings, which are well known and are easily exploitable).



The Plugins category is the second risk factor in a WordPress website. A common misconception is that the website will be safe as long as your plugins are up to date.

Plugin updates can be easily automated and are promptly applied as soon as a new version of the plugin is released by the vendor. However, there are inherent vulnerabilities even to their newest versions.

A valuable example is the famous WooCommerce Leak of 2001 that exposed 5 million websites to theft.

WooCommerce is a popular e-commerce platform for WordPress online stores, handling online stores and their payments. Hacker News estimates that in 2023 WooCommerce is installed on over 600,000 websites.

In 2021 it was found that several of its components were vulnerable to SQLi and were left unpatched through different versions, resulting in an attack spree.

In such cases, automated updates and breach detection are of little help: a solid security strategy that can prevent these attacks can make the difference, instead.

Hardening and properly configuring other website components will greatly help prevent breaches and mitigate the exposure of the website to an attack.

III. Understanding the impact of a data leak or a hacking attack

According to the **IBM Cost of a Data Breach Report 2023**, the global cost of a data breach in 2023 was **USD 4.45 million**, with a **15% increase** over three years.

The same report highlights how 51% of the organizations is planning to increase their security investments as a result of a breach.

This indicates that they are in a reacting mindset rather than preventative.

Indeed, it seems that most companies are willing to roll the dice on the chances of a hacking event, largely underestimating the impact of a data breach and the ripples that it causes through the supply chain.



We can summarize the impact of a data breach as follows:

- ▶ Financial Impact
- ▶ Reputational Damage
- ▶ Operational Impact
- ▶ Collateral impact to Individuals and the supply chain

FINANCIAL IMPACT

Financial Impact is often the only risk factor taken into account by organizations. It manifests itself in terms of:

- ▶ **Data breach costs:** this includes the cost of notifying affected customers, investigating the breach, and implementing security measures to prevent future breaches.
- ▶ **Loss of revenue:** a hacked website may be shut down or blacklisted by search engines, which can lead to a loss of revenue. Additionally, businesses may lose customers if they believe that their personal information is not secure.
- ▶ **Legal fees:** businesses that suffer a data breach may be subject to lawsuits from customers, employees, or regulators. These lawsuits can be costly, even if the business is not found liable.

REPUTATIONAL DAMAGE

The reputation damage ensuing a data leak can bring to equal, if not superior, losses to a business in terms of:



- ▶ **Erosion of trust:** a data breach or hacking attack can damage a business's reputation and erode trust with customers. This can make it difficult to attract new customers and retain existing ones.
- ▶ **Negative publicity:** A data breach or a hacking attack can make the headlines, which can further damage a company's reputation.

OPERATIONAL IMPACT

Operational damage must also be taken into account, in the form of:

- ▶ **Downtime:** a hacked website may be taken offline, disrupting business operations and productivity.
- ▶ **Security Costs:** after an attack, a business will likely invest in additional security measures such as hiring security personnel, purchasing security software, and upgrading their hardware to prevent future attacks.
- ▶ **Distraction from Core Business:** responding to a data breach or hacking attack can be a major distraction for businesses, taking time and resources away from core business activities.



COLLATERAL IMPACT TO INDIVIDUALS AND THE SUPPLY CHAIN

Besides the direct costs to the business, there are also collateral damages to the individuals whose data was stolen.

Hackers can steal personal information such as names, addresses, and social security numbers to commit identity theft or to resell them to larger criminal organizations in the dark web.

Stolen financial information can be used to open fraudulent accounts, make unauthorized purchases, and commit other types of financial fraud. Restoring credit and financial reputation after such an event may take months (if not years) and have important repercussions on the victim and their families.

As a result, victims of data breaches and hacking attacks are likely to experience emotional distress, such as anxiety, fear and anger, and have lasting consequences including losing trust in businesses and online services.

MULTI-PARTY BREACHES


While many attacks are carried out as independent episodes, when it comes to new vulnerabilities, it's likely that attacks will not be isolated.

In a 2019 research study from RiskRecon and Cyentia Institute, multi-party breaches have an average **x10** the financial damage of a traditional single-party breach.

The rippling effects of such an event takes an average of **379 days** to affect 75% of its downstream victims.

The study also reports that the largest ripple in terms of organizational impact affected **550 firms**.

This is why conducting regular vulnerability assessments can provide a number of benefits, including:

- 
- ▶ Proactively identifying and addressing security vulnerabilities
 - ▶ Reducing the risk of successful attacks
 - ▶ Building trust with customers and partners
 - ▶ Complying with industry regulations.

By implementing a comprehensive vulnerability assessment program, businesses and individuals can take a proactive approach to website security and protect their valuable data and assets.

IV. Vulnerability assessment methodologies

A website vulnerability assessment is a critical process that identifies and analyzes potential weaknesses in a website's security posture. This helps businesses and individuals proactively address security concerns before they are exploited by attackers.



To do that, different techniques can be used, including network scanning, host scanning, web application scanning, manual penetration testing, and source code review.

There are a variety of automated tools available – either commercially or open source – that can perform most of these. These tools can scan websites and identify vulnerabilities, generate reports, and prioritize remediation efforts.

The best vulnerability assessment techniques for a website will depend on a number of factors, including the size and complexity of the website, the budget available, and the level of risk tolerance.

When it comes to WordPress websites specifically, the attack surface is constituted by WordPress specific components and its underlying environment and configuration.

Checking on WordPress-specific components with out-of-the-box tools is essential, but doing **just that means doing only half the job.**

Besides Core, Plugins, and Themes, a comprehensive WordPress security routine should assess other aspects that are inherent to the website daily cycle, such as backups and user management.

An all-round security strategy should also include how to maintain security in common real-life case scenarios within the WordPress website lifecycle with a heightened risk.

This is the case of using specific outdated versions of a plugin, using a theme that gets discontinued, using a provider that imposes administrative restrictions, or the necessity to migrate a website to a different server.

It is therefore important to use a combination of different techniques to get a complete picture of the websites' security posture.

When it comes to choosing manual vulnerability techniques or automated routines, different aspects must be considered.

MANUAL VULNERABILITY ASSESSMENT

A manual vulnerability assessment is a detailed and comprehensive process that involves a security analyst or team thoroughly examining a website's code, configuration, and network for vulnerabilities.

This type of assessment is typically more expensive and time-consuming than automated assessments, but it can also be more effective at identifying complex vulnerabilities that automated tools may miss.

ADVANTAGES

- ▶ More in-depth and comprehensive
- ▶ Can identify complex vulnerabilities
- ▶ Can provide more context and insights



DISADVANTAGES

- ▶ More expensive and time-consuming
- ▶ Requires specialized skills and knowledge
- ▶ Not as scalable as automated assessments

AUTOMATED VULNERABILITY ASSESSMENT

An automated vulnerability assessment uses software tools to scan a website for vulnerabilities. These tools can quickly scan large websites and identify common vulnerabilities, such as SQL injection, cross-site scripting (XSS), and outdated software.

Automated assessments are typically less expensive and time-consuming than manual assessments, but they may not be as effective at identifying complex vulnerabilities.

ADVANTAGES

- ▶ Less expensive and time consuming
- ▶ Can scan large websites quickly
- ▶ Can identify common vulnerabilities



DISADVANTAGES

- ▶ May not be as effective at identifying complex vulnerabilities
- ▶ May generate false positives
- ▶ May not provide as much context and insights as manual assessments

We have summarized the Pro’s and Con’s in the table below:

| Feature | Manual Assessment | Automated Assessment |
|---|---|---|
| Depth and comprehensiveness | Is more in depth and comprehensive | Scans for the most common components |
| Effectiveness at identifying complex vulnerabilities | Is more effective | Is less effective |
| Cost | Is more extensive (depending on the scope, it averages around \$2,500 USD) | Is less expensive (a few hundred dollars a year) and may also be free for a limited number of scans or targets |
| Time consumption | Is more time consuming (it may take from a few days to a few weeks) and may require multiple resources with different skillsets | Is less time consume (may require from a few minutes to a few hours) |
| Skill and knowledge required | Requires special skills and knowledge | Doesn’t require special skills and knowledge to execute, but it might require them to interpret and analyze the results to make them actionable |
| Scalability | Isn’t easily scalable | Allows for a scalable strategy |

Which method is right?

Striking the right balance when assessing a website’s security posture can be daunting.

At Negative PID, we have elaborated a strategy to obtain the best of both worlds and minimizing the downsides.



V. Rationale for automating vulnerability checks in WordPress

The challenges of manual assessments are costs, time, and scalability. As we have mentioned before, the WordPress ecosystem consists of thousands of components and integrations, built with multiple technologies that go way beyond PHP and HTML. All these components are updated with a tight calendar (weekly or even daily) to apply patching as soon as possible to the constantly evolving threats.

A manual assessment for WordPress components is unlikely to be cost effective, timely, and error-free. Its findings risk indeed to be outdated by the time the report is delivered to the customer.

Therefore, automation seems a necessity more than a choice to produce accurate and actionable results.

On the other side, the benefits of automation are often offset by its limitations. Indeed, running an automated check on limited components can return a reassuring outcome and induce a false sense of security even if it is conducted on limited components and products.

Another set of challenges in WordPress vulnerability assessments is the type of information and analysis offered by open source tools. While many tools are extremely efficient in probing and obtaining information, they lack in analysis, context, and explanation. This is why manual vulnerability checking reports typically take a long time to compile.

Our approach to solve these problems has been a modular one:

1. We have created a comprehensive security routine that is tailored to WordPress websites, their underlying eco system, their configurations and common real-life life-cycle scenarios.
2. We have automated these routines by creating our own scripting for gathering information with a modular strategy. We have excluded the analysis from the automation.
3. We have used data science and a statistical language to bring all the harvested information together, analyze it, cross-reference it with multiple authoritative sources, contextualize it, and produce an automated report tailored on its specific findings.

4. We have integrated a secure service for storing our reports and sharing them with our customers with end-to-end encryption and in compliance with the strictest security standards such as ISO, HIPAA, and GDPR.

Our service is ultimately broken down into three modules:

- ▶ **Information gathering**
 - ▶ Kali Linux and Parrot Security
 - ▶ Bash scripts
 - ▶ OSINT framework
- ▶ **Data analysis and reporting**
 - ▶ R Studio Server on Debian
 - ▶ R, R Markdown
 - ▶ R Studio
- ▶ **Secure storage and data transmission**
 - ▶ Proton Drive and Proton Mail
 - ▶ Bash scripts
 - ▶ End-to-end encryption



There are several benefits to this approach:

- ▶ Kali Linux and Parrot Security tools enable comprehensive information gathering through different powerful tools that can mostly be operated from the command line.
- ▶ Automated bash scripts with a modular execution model allow for flexibility and a manual assessment-like experience, at a fraction of the time, and with an easily scalable model over multiple machines.
 - ▶ Data science with R is a powerful and quick way to manipulate non-rectangular data in JSON, XML, and HTML formats. The R framework also provides packages for extracting, standardizing, and cross-referencing data for detailed custom analysis.
 - ▶ R Markdown connects our R code, analysis results, and commentary by parsing them into a single, nicely formatted document. Creating custom reports based on the results of our data analysis and exporting it



into HTML or PDF format is what enables the efficiency of the entire process.

- ▶ Once the final report has been created, the integration with Proton Drive and Mail allows for secure end-to-end and at rest data encryption. This allows for a secure storage and transmission of the documents to our customers. It also reduces the costs of producing hard copies and shipping time, while maintaining the information safe at all times.



All in all, **our strategy allows us to maintain the advantages of human assessment, while maximizing the advantages of automations.**

VI. Building an automated vulnerability testing framework in R

Building an automated WordPress vulnerability testing framework in R might seem like an odd choice. However, **R revealed to be an asset in most stages of our security routine.**

Packages like [ProcessX](#), [System](#), and [System2](#) allow the execution of system commands and processes within the same R script. This is an extremely efficient way of building an ad-hoc interface for our automations.



The most obvious use for R scripting is for data manipulation and analysis. The manipulation capabilities of R on non-rectangular structures and data extraction enabled us to scan large amounts of data with keywords and strings for the detection of headers, plugins, versions, users, and much more.

The granular control over these searches are what allow us to build on the existing modules, improve them at need, and implement new features at speed.

Finally, the powerful R Markdown framework allowed us to transform the results into an easy-to-read report whose sections and commentary populate according to the results retrieved. This allows us to compile pertinent and relevant reports in just minutes. The reports are easily exportable to HTML or PDF format, ready to be shared with the customer.



All in all, the use of R tools in combination with Kali Linux and Parrot Security tools were key to delivering a report with the accuracy of a manual vulnerability check in less than 48 hours from the order, including manual review and some contingency for existing workloads.



VII. Case studies and use cases

In July 18, 2023 Hacker News reported an insightful article on another WooCommerce flaw enabling unauthenticated attackers to impersonate arbitrary users and perform administrators actions, thus allowing for the website takeover.

The flaw can be tracked as [CVE-2023-28121](#) with a [CVSS risk score of 9.8](#).

WordFence reported that in the month of July, this vulnerability led to large-scale attacks ([1.3 million attacks over a weekend](#)) against [157,000 websites](#) implementing the WooCommerce Payment plugin versions 4.8.0 through 5.6.1.

The common denominator for these attacks was the use of a specific header identifying the plugin with an embedded user tag for admin users. This allowed the attacker to treat additional payloads (such as the deployment of a backdoor) with admin privileges.

In cases like this, the knowledge of a plugin flaw spreads very quickly over the hackers community. As the chart below provided by WordFence shows, the scans for that specific header spiked very quickly over a few days, and eventually resolved as the patch for the two interested plugins was released and users updated to the latest version.

WordPress attacks interesting plugins and other integration components escalate quickly, but can typically be resolved with repeated scans and constant updates.

In the case of the WooCommerce Leak of 2001, instead, the impact was much worse because the attacks could only have been mitigated by an existing good security posture.



Our WordPress Vulnerability Assessment service aims at providing our customers with the tools to be prepared in both scenarios.

Hardening the environment hosting the website requires more effort, but it mostly constitutes a one-time effort with minimum maintenance and adjustments. On the contrary, WordPress-specific components like plugins need constant updating and assessment.

This is why our service provides help and guidance of both sides and is available in different formats for different use cases.

VIII. Best Practices for WordPress Security

Adopting best practices for WordPress security can go a long way in preventing attacks and data breaches. This is why our reports provide specific best practices for the different tested areas and strategies to include WordPress security in your existing routines. We do that in compliance with the strictest security standards, such as [ISO](#) and [SOC 2](#).

In general, we recommend the following best practices to any WordPress website owner:

1. [Keep WordPress updated](#): WordPress regularly releases security updates to fix vulnerabilities. It is important to keep your WordPress core, themes, and plugins up to date to ensure that you are protected against the latest threats.
2. [Use strong passwords](#): A strong password is essential for protecting your WordPress website. Use a combination of upper and lowercase letters, numbers, and symbols, and avoid using easily guessable information such as your name or birthday.
3. [Enable two-factor authentication \(2FA\)](#): 2FA adds an extra layer of security to your WordPress login by requiring you to enter a code from your phone in addition to your password. This makes it much more difficult for attackers to gain access to your website.
4. [Choose a secure hosting provider](#): Your hosting provider plays a critical role in the security of your WordPress website. Choose a hosting provider that has a good reputation for security and that offers features such as malware scanning and automatic backups.



5. **Limit login attempts:** Limiting the number of login attempts that can be made within a given period of time can help to prevent brute-force attacks. You can use a plugin such as Login LockDown or Limit Login Attempts to implement this.
6. **Install a security plugin:** A security plugin can help to protect your WordPress website from a variety of threats, such as malware, phishing attacks, and SQL injection. Some popular security plugins include Wordfence, Sucuri Security, and iThemes Security.
7. **Change your default admin username:** The default "admin" username is a common target for attackers. Changing your admin username to something unique will make it more difficult for attackers to guess your login credentials.
8. **Disable file editing:** Disabling file editing in the WordPress dashboard can help prevent attackers from modifying your website's files. You can use the WP-File-Editor plugin to disable file editing.
9. **Back up your website regularly:** Regularly backing up your website can help you to recover from a data breach or other security incident. You can use a plugin such as BackUpWordPress or UpdraftPlus to back up your website.
10. **Keep your contact information up to date:** Making sure that your contact information is up to date can help you to receive security notifications and updates. You can update your contact information in the WordPress dashboard under Settings > General.



IX. Conclusion

In today's digital age, security is no longer an option; it's a necessity. With the ever-increasing threat of cyberattacks, it's crucial that businesses and individuals take steps to protect their data and assets.

Protect your data: Your data is your most valuable asset, and it's essential to safeguard it from unauthorized access, theft, or corruption.

Prevent cyberattacks: Cyberattacks can cause significant financial and reputational damage. Implementing robust security measures can help you prevent these attacks from happening in the first place.

Keep your customers' trust: Customers trust you with their personal information, and it's your responsibility to protect it. Implementing robust security measures can show your customers that you take their privacy seriously.

To do that, conduct regular security assessments. Regularly assess your security posture to identify and promptly address and remediate vulnerabilities. Adopt an integrated and holistic approach to security: checking for specific WordPress components is just not enough.

The cost of a data breach can be devastating, for small and large businesses alike. Implementing robust security measures now can help you avoid these costs in the future.

Take action today: don't wait until you're attacked to start thinking about security.

Contact us today to discuss how we can help you implement robust security measures for your business. At Negative PID we have designed a system of initiatives to reward your adoption of solid security routines and to accompany you in your journey towards security... and peace of mind.

<https://negativepid.com>