The Future Is the Web! How to Keep It Secure?

OCTOBER 2019

acunetix

Contents

Introduction

The Future Is the Web!

HOW TO KEEP IT SECURE?

Web technologies are the core of the Internet. They are already adopted by email, communications, mobile applications, and more. They are making their way into innovative solutions such as the Internet of Things. To keep your enterprise secure, you need to build a strategy that includes securing the web. Since security experts are becoming a scarce resource, your greatest allies in this are automation and integration.

Web Technology Adoption

The application layer used to be mostly static assets like marketing websites, but flash forward to today, it is now often the primary way an enterprise interacts with their customers. With this massive shift in functionality comes an equally massive shift in risk.

Zane Lackey
Signal Sciences

The days of simple web pages are long gone. When Tim Berners-Lee introduced us to this technology, he probably never imagined how far it would go. At first, the web was there just to publish information easily. Now, no company can afford to miss out on fully-fledged web presence. And this no longer means just posting a company logo and a contact form.

In the Forbes report called ***"60 Cybersecurity Predictions for 2019"***, Zane Lackey of Signal Sciences states: *"The application layer used to be mostly static assets like marketing websites, but flash forward to today, it is now often the primary way an enterprise interacts with their customers. With this massive shift in functionality comes an equally massive shift in risk."*

The number of websites has a tendency to grow exponentially from year to year. For example, according to Internet Live Stats, the number of websites in 2017 was almost twice that of 2016. At the moment, there are approximately 2 billion unique publicly available websites. This means 2 billion potential points of entry for criminals.

The growing complexity of web interfaces means that they are more difficult to secure. Their rising popularity means that cybercriminals are more inclined to use them as entry points. The increasing integration and move to the cloud mean that more and more systems are interconnected. As a result, there are more and more cases when a successful web attack may lead to full system compromise and give the attackers access to critical data.

The problem with web vulnerabilities is that they are not discovered by general security tools and typical protection tools such as firewalls are helpless against them. This means that to secure the web, enterprises must know exactly what tools to use and must be able to include these tools in their complex and comprehensive security systems. Unfortunately, many of those tools still require a lot of manual intervention.

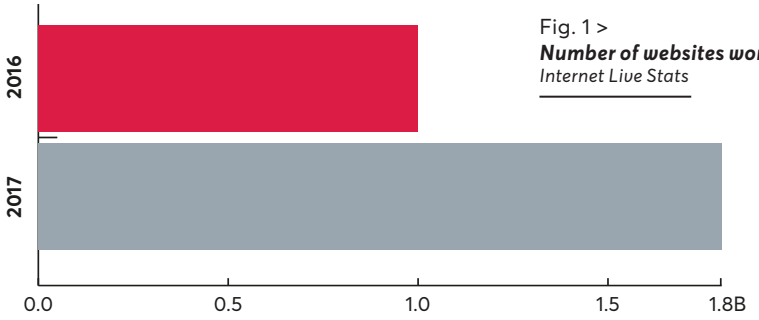


Fig. 1 >
Number of websites worldwide
Internet Live Stats

The World Is Open Source

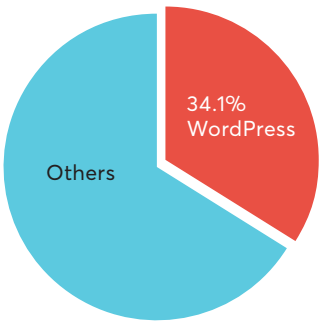
It is hard to find a website or web application that uses no open source at all. Even custom-made solutions often use open source libraries. According to W3Techs, WordPress alone is currently used by 34.1 percent of websites worldwide and this number is expected to increase based on current trends. For example, by the end of 2017 WordPress was used by 29.2 percent of websites.

While open-source web software has many advantages, it also introduces major risks. If a web vulnerability is discovered in an open-source system or library, it may introduce a huge attack surface. For example, according to ZDNet WordPress sites accounted for 90 percent of all hacked CMS sites in 2018. This means that you must continuously monitor your open source solutions for vulnerabilities.

What's worse, many businesses fail to keep their open-source software up to date. For example, according to The SSL Store, 33% of top WordPress sites in 2018 were at least two versions behind. This means that many businesses are not only failing to keep their systems secure but they most certainly do not use vulnerability monitoring software at all, leaving an open door for criminals to enter.

There are several reasons why businesses choose not to monitor their open-source websites. For some, it may be due to lack of information. Businesses without dedicated security teams may not realize that their "comprehensive" security solutions fail to protect against web attacks. Other businesses choose not to implement web vulnerability protection because most tools are difficult to integrate with their other systems.

Fig. 2>
Software used by websites



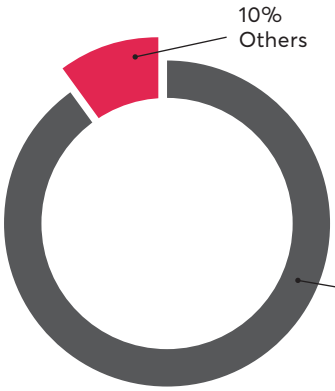


Fig. 3>
Hacked CMS sites / 2018

While open-source web software has many advantages, it also introduces major risks. If a web vulnerability is discovered in an open-source system or library, it may introduce a huge attack surface.

Shift to Mobile

The current generation is the mobile generation. You can hardly imagine a person nowadays who does not use a smartphone or a tablet. Many use such devices much more often than desktop computers or laptops.

Businesses with web applications cannot ignore this trend and mobile technology users don't want to visit regular websites. That is why businesses must introduce dedicated mobile applications. In most cases, these applications are just simple interfaces to the websites or provide exactly the same services.

However, almost all mobile applications communicate with back-end systems using web technologies. They are based on web APIs (primarily REST), which use the same communication protocols and architectures as regular web applications. This means that such mobile interfaces are just as susceptible to web vulnerabilities as regular websites.

Businesses fail to protect their web APIs for similar reasons to those that fail to protect their web applications. Primarily, they are not aware that it is needed. And even if they are aware, they find that most current software is too complex to use for that purpose.

Almost all mobile applications communicate with back-end systems using web technologies. This means that they are just as susceptible to web vulnerabilities as regular websites.

Internet of Things

Many sources predict that 2019 and onwards will be the years when the Internet of Things will succumb to the dark side. For example, Forbes included IoT as one of the five key tech trends driving cybersecurity in 2019. We already have smart TVs, smart home systems, and more technologies such as smart cars are just around the corner. However, security is not too good when it comes to these emerging technologies.

In the 2019 Forbes report, Uri Rivner from BioCatch states: *"Your smart fridge will start scamming you. IoT-connected appliances such as refrigerators and washing machines already produce unattended payments that the user cannot personally verify. Fraudsters see this vulnerability now and will begin to take advantage of it."*

Your smart fridge will start scamming you. IoT-connected appliances such as refrigerators and washing machines already produce unattended payments that the user cannot personally verify. Fraudsters see this vulnerability now and will begin to take advantage of it.

Uri Rivner > **BioCatch**

Talent Shortages

The number of assets that may be vulnerable keeps rising. The complexity of systems to protect keeps increasing. The potential attack surface keeps growing. However, one thing seems to show quite the opposite trend: the availability of cybersecurity talent is diminishing.

The Cybersecurity Ventures Cybersecurity Jobs Report 2018-2021 predicts that there will be 3.5 million cybersecurity job openings by 2021. *"Every IT position is also a cybersecurity position now. Every IT worker, every technology worker, needs to be involved with protecting and defending apps, data, devices, infrastructure, and people. The cybersecurity workforce shortage is even worse than what the jobs numbers suggest."*

In the 2019 Forbes report, Jason Albuquerque of Carousel Industries states: *"It's no surprise that we are currently in a massive deficit of qualified cybersecurity talent. In 2019, we will see a more modern approach to recruiting and retention in the cybersecurity workforce to fill this void and create more diversity. We will see an uptick in apprenticeship programs, more diverse training, recruiting practices and federal funding to help bridge the enormous talent and diversity gap the industry has today."*

However, these actions most probably won't be enough to fill the gap. Cybersecurity personnel will become extremely valuable with businesses having to try very hard to retain their security experts because if they lose them, they will not be able to find more. There are two things that businesses can do to help it: automate as much security work as possible and keep their security personnel interested in their job by not giving them mundane tasks.

It's no surprise that we are currently in a massive deficit of qualified cybersecurity talent. In 2019, we will see a more modern approach to recruiting and retention in the cybersecurity workforce to fill this void and create more diversity. We will see an uptick in apprenticeship programs, more diverse training, recruiting practices and federal funding to help bridge the enormous talent and diversity gap the industry has today.

Jason Albuquerque
Carousel Industries

The Perfect Solution

In the web security industry, there is an ongoing shift from simple manual tools to business-class software. There are many tools on the market that can be used for manual processes. However, there is a small number of solutions that approach the problem from a business point of view. To invest in the future, choose tools that focus on automation and integration and that will grow with your company.

Replacing Manual Processes

The number of websites grows not just worldwide but also within organizations. This might not be a problem for small, local businesses, but can be a major headache for large, international corporations. Keeping physical resources secure is easier because these resources need to be purchased, installed, and it's difficult to overlook them. However, virtual resources present a bigger problem: in a large organization, it's not uncommon to overlook a new, publicly accessible asset.

For example, imagine a multinational corporation with offices in different countries, where a local marketing department decides that they need a temporary website for a local campaign. Since it is easy to set up a simple WordPress site, all they need to do is to ask their local administrator for a subdomain and hosting site access.

However, if web security is handled by a different unit, for example in a different country, that unit might not always get informed about the new website. Even if manual processes exist that require the administrator to report each new website, it may be overlooked. As a result, such a website may not be included in web security scanning. Even if it does not contain any valuable resources on its own, it may be the first point of entry for an attacker if it's not kept secure.

There is a simple solution to eliminate a manual reporting process for new websites and to avoid such errors. It involves using web crawlers similar to those employed by search engines. Such crawlers may use different techniques such as DNS lookups and SSL certificate analysis to find all new websites that belong to a company. There are now web security solutions on the market that use this search-engine technology to continuously discover new web assets.

This approach eliminates several problems: it reduces the manual workload for administrators and security officers, it removes the need for a manual process, and it reduces the potential attack surface. Therefore, a decision about whether to employ such a tool in a large organization is obvious: it is worth it.

Indispensable Issue Tracking

Nowadays, it is hard to imagine any development team that would not use some kind of an issue tracking solution. These may be standalone solutions such as the very popular Jira or a comprehensive platform bundled together with version control such as GitHub or GitLab.

When compared to software development, web security solutions often seem, unfortunately, very primitive. There are tools that include some kind of internal issue tracking

but many products don't work too well with other systems. Therefore, a security team is forced to perform a lot of work manually, which is not only prone to error but a huge waste of time for such scarce and valuable human resources.

If a penetration tester uses a simple standalone web security scanner and finds a security issue, it only marks the beginning of a critical process: fixing the vulnerability. This often means that the security researcher must manually enter the details of the vulnerability into the issue tracker so that the issue may be taken over by the development team.

This means unnecessary manual work for a valuable resource and there is often no feedback! If the development team believes that they eliminated the vulnerability, they simply close the issue. But what if the issue is only partially fixed and the vulnerability still exists? It would have to be randomly picked by the penetration tester at some other time.

Again, there is a very simple solution to this problem based on automation and integration. However, only some of the web security tools available on the market make it possible. A business-class security tool should work together with the issue tracker in two ways. First of all, it should be able to automatically create issues. This includes assessing the impact of the vulnerability (so that correct severity can be set in the issue tracker) and assigning it to the right team automatically. Second of all, it should automatically retest the application after the issue is marked as fixed by the developer and reopen it if the vulnerability persists.

With such integration, the penetration tester does not have to be involved at all. The web security scanner finds typical vulnerabilities, automatically reports them, and prevents them from persisting by reopening unfixed issues. This keeps the penetration tester happy because they can spend their time doing something important instead of filling out bug reports. And this keeps the applications secure because they cannot be marked as fixed unless they are really fixed. It's a win-win situation.

The Age of DevSecOps

Security solutions must follow in the tracks of innovation in the world of software development. The days of manual software testing are long gone. In the past, developers used to submit and compile new code manually and testers used to (also manually) follow test cases and test suites, painstakingly clicking the screen and entering test data to check if everything works as intended.

Now, manual tests are replaced with automated solutions as much as possible and manual testers get promoted to test designers/engineers. Solutions such as Selenium imitate human actions, doing the automated clicking and data entering every time new code is committed and compiled. Complex Continuous Integration solutions such as Jenkins are automating the whole process.

As a result, the developer needs to just commit new code to Git and forget about it. The CI solution performs the whole process automatically: creates a temporary container, compiles the application (and checks if it compiles correctly), and runs the test suites. If anything fails, the developer is informed so they can correct the code and commit it again. This whole process is overseen by DevOps engineers who build such automated processes and monitor them.

However, security-conscious companies don't just have DevOps, they have DevSecOps. This means that automated processes include security checks as well. For this, DevSecOps need tools that can work just like Selenium but for vulnerability scanning. That is why a business-class web security solution should be able to work together directly with a CI platform.

Web security software manufacturers are more and more aware of that need and several web vulnerability scanners have simple options to include security scans in these processes. However, business-class solutions must be able to go further, they can't just offer simple pass or fail conditions. A scanner that integrates with a CI solution must be able to automatically assess the vulnerabilities

found and provide suitable information to the developer so that they may easily fix it before committing code again. It must also work fast so that CI processes don't take ages.

Again, including security scanning in Continuous Integration processes is a win-win situation. If web security is checked only by running night scans on production websites, it may introduce huge costs and unnecessary risks. After all, before new software (either in-house or third-party) makes it to production, it can be verified at multiple stages: user acceptance testing, staging, QA, but most importantly: at the development stage. The added bonus is the fact that this does not involve valuable cybersecurity human resources at all!

The Perfect World

Let us imagine the perfect world of enterprise web security. If the right solution is implemented and integrated, the penetration tester can completely skip mundane tasks. Most vulnerabilities are discovered as soon as the developer introduces them, automatically monitored and fixed. Regular scans guarantee that current software is safe even if new vulnerabilities are discovered by the general hacker community.

Does that mean that high-skill penetration testers are no longer needed? Quite the opposite! High-skill penetration testers follow that career path because they enjoy a challenge. They do not become security experts to fill forms or replicate what has already been discovered. They want to spend their time getting deep into code/applications and finding things that nobody else found yet. This keeps them happy with their job and this is what businesses hire them for – to be one step ahead of black hat hackers.

The Perfect Product

To keep your websites safe and to retain your valuable personnel, you must employ the right solutions. And one of these solutions is Acunetix 360.

Acunetix 360 addresses all the concerns mentioned above. It uses search engine technologies to continuously discover enterprise assets so that no web application or website remains unprotected. It also has two-way issue tracker integration capabilities: it creates issues, assigns them to the right people, and reacts to issue status changes by initiating verification scans.

Acunetix 360 is also built for integration with the software development lifecycle (SDLC) and supports multiple CI/CD solutions (Continuous Integration / Continuous Delivery). Because Acunetix 360 uses the trusted Acunetix vulnerability scanner engine it is also one of the fastest and most precise tools on the market. Additionally, the Acunetix vulnerability scanner engine is a product that has been continuously improved for nearly 15 years, making it the most established solution on the market.

About Acunetix

Acunetix is a global web security leader. As the first company to build a fully dedicated and fully automated web vulnerability scanner, Acunetix carries unparalleled experience in the field. The Acunetix web vulnerability scanning platform has been recognized as a leading solution multiple times. It is also trusted by customers from the most demanding sectors including many fortune 500 companies.

Our mission is to provide you with a trustworthy web security solution that protects all your assets, aligns with all your policies, and fits perfectly into your development lifecycle. The Acunetix platform frees up your security team resources. It can detect vulnerabilities that other technologies would miss because it combines the best of dynamic and static scanning technologies and uses a separate monitoring agent. It is your platform of choice for comprehensive web vulnerability assessment and vulnerability management.

acunetix

WHERE TO FIND US

Stay up to date with the latest web security news.

Website. www.acunetix.com

Acunetix Web Security Blog. www.acunetix.com/blog

Facebook. www.facebook.com/acunetix

Twitter. twitter.com/acunetix

CONTACT INFORMATION

Acunetix (Europe and ROW)
Tel. +44 (0) 330 202 0190
Fax. +44 (0) 30 202 0191
Email. sales@acunetix.com

Acunetix (USA)
Tel. (+1) 737 241 8773
Fax. (+1) 737 600 8810
Email. salesusa@acunetix.com