SECURITY
by HTTPCS

VULNERABILITY SCANNER
WEB & APPLICATIVE

- **0 false positive** guaranteed
- **100% Mapping** & **Headless** Technology
- Automated **Black Box** and **Grey Box** audits
- **Zero-Day Vulnerability** management
- **Machine Learning** based solution

> For Sanofi's websites, we were looking for a vulnerability scan in SaaS mode. We chose Security for **the ergonomics of the dashboard** which allows to **get started fast,** as well as for its ability to **export the results according to diverse criteria** and for its **continuous monitoring** technology, based on an evolutive analysis.
>
> Security by HTTPCS is an efficient solution which allows us to manage a large scope of several hundreds of websites with a reasonable cost and an excellent operational and business relationship.

SANOFI

Wilfried **LAUMOND**,
ITS Cyber Security / Risk Monitoring & Services
Information Technology & Solutions

SECURITY
by HTTPCS

KEY ADVANTAGES
PRODUCT FEATURES

ZERO-FALSE-POSITIVE GUARANTEED

HTTPCS guarantees **zero-false-positive audit reports**, as evidenced by the Simulation button, allowing the user to r**edo the simulation attack**. A conclusive evidence that the flaw could be exploited by hackers.

SOLUTION BASED ON MACHINE LEARNING

The HTTPCS scanner robot **learns continuously** from the paths already tested during previous audits to r**efine its attacks scenarios** to detect new flaws. It is not based on fingerprint but on an attack scenarios knowledge base.

HEADLESS AND 100% MAPPING TECHNOLOGY

Thanks to the use of the Headless technology, the HTTPCS robot is **able to scan 100% of a website map**, including dynamic contents such as JavaScript. Two modes are available: **Grey Box** (with login details, several types of authentication supported such as SSO) and **Black Box** (without login details).

0-DAY EXPLOITS DETECTION

The HTTPCS cybersecurity experts perform a **daily watch** over the different levels of the Internet to keep the robot's knowledge base up to date with **OWASP Top10, CVE and the new 0-day exploits.**

ADDITIONAL ADVANTAGES

✓ Flawless responsiveness and flexibility

The HTTPCS team takes into account **client's feedback** to continuously improve its solutions (interface, features, technology, support...).

✓ A smooth and ergonomic 100% SaaS interface

The user experience is helped by an **user-friendly and easy-to-use** interface, conceived to facilitate security scans management and vulnerability reporting (filters, categories, PDF Export, qualification of criticality). The interface is available in **several languages** including French and English.

✓ Scans of preproduction environments

The HTTPCS scanner allows to scan **all preproduction environments** to correct the flaws before the production deployment of a website or a web application.

✓ Offensive Cybersecurity

The HTTPCS scanner is an **offensive cybersecurity solution** which **goes way beyond** simple defensive solutions such as **WAF or IDS.**

✓ Compatible with all CMS

HTTPCS scans **all websites created from CMS**, such as WordPress or Drupal.

✓ API available upon request

Allows to ease interconnections **with other solutions**, upon request without surcharges.

✓ No setup fees

Free installation, no training needed, the technical **support is completely free** and available in 8 languages.

✓ No need for any cybersecurity expertise

The HTTPCS interface was conceived to be u**sed by any professional**, even the ones with no cybersecurity skills.

✓ Advanced User Management

User right management console available upon request (fee-paying option): allows to **define different rights** for a large number of users for an easy large-scale management.

THE CYBERSECURITY CERTIFICATION SEAL BY HTTPCS

The Cybersecurity certification seal by HTTPCS is a token of trust to display on an ecommerce website. It reassures the web users and allows you to differentiate yourself from competition with the guarantee that your website is secured (brand image, e-reputation).

PRODUCT OVERVIEW

Short presentation of ZIWIT

Since 2011, ZIWIT is an expert in **offensive cybersecurity.** Headquarted in Montpellier (France) where all data are hosted, Ziwit is **the European leader** in offensive security and works with more than 9.000 companies worldwide, including **major international groups** such as Sanofi or Adobe.

ziwit

3 expertise areas

ZIWIT has developed around a team comprised of **cybersecurity experts** and **white hats,** allowing us to support companies through three expertise areas:

- ✓ **Editing** of the offensive cybersecurity automated **suite** HTTPCS.
- ✓ **Customized consultancy services**: Manual security and compliance audits, penetration tests, emergency interventions for incident response or forensic.
- ✓ **Cybersecurity training centre:** Technical training, awareness sessions, compliance (GDPR...), transfer of skills.

Detailed key advantages of SECURITY by HTTPCS

TECHNOLOGY & MACHINE LEARNING

The **next generation** vulnerability scanner SECURITY by HTTPCS scans the websites and web applications by simulating hackers' behaviour and performs **attacks scenarios** to identify all types of flaws (non-limited to OWASP Top10 and CVE, frequent updates of the database with 0-day exploits).

Based on machine learning, it refines **daily its attacks scenarios** to identify new flaws. We highly recommend using the solution at least for a period of **30 days in a raw** (technology optimization).

It audits 100% of the web tree via **black box (without login details) and grey box (with login details)** tests. It allows the robot to expand its attack area. It audits also dynamic content thanks to an embedded JavaScript engine.

COMMENTS & SEAL

It is possible to **leave a comment** for each flaw and to send the details of a specific vulnerability by email to your team and / or your services provider (for remediation). You may **define categories** and prioritize the correctives to adapt the use of the robot to your organization (in case of sensitive websites to focus on for example).

Finally, you can display the HTTPCS certification seal on each page of your website: it shows the date of the last flawless audit, to ensure the web users **that your website is completely secured** (e-reputation, brand image...).

ATTACK SIMULATION

The flaws can be checked thanks to **the "Simulation" button**, available on the reports (the simulation does not impact your website or web application). This button allows to simulate the attack on your website (until the flaw is corrected) and to **better understand the incurred risks**.

REPORTS & REPORTING

The reports are **exportable into PDF** and include a server review (reverse IP, open ports, SSL certificates...), as well as the configuration good practices to adopt.

The robot detects automatically whenever a flaw is corrected (the flaw is tagged as corrected after 3 successive audits), allowing an **efficient reporting of your remediation actions**.

ZERO-FALSE-POSITIVE

After each audit, the robot generates a **zero-false-positive guaranteed report** where only trusted flaws, that is flaws exploitable by hackers, are listed (no need for manual reprocessing, time-saving advantage for analysis and remediation). The report includes also the **countermeasures** to apply, the **details of each flaw**, their **level of criticality** (CVSS V3 score), the incurred risks and the ISO 27001-27002 standards impacted.

KEY ADVANTAGES OF THE HTTPCS CONSOLE

- ✓ Automated, autonomous and **global management** of your web and system applicative security by our robot
- ✓ Easy-to-use & simple **access and reporting**
  - → **No cybersecurity skills required** to be informed of your website's vulnerability
- ✓ **Unlimited automated alerts** by email or text messages for a real-time monitoring even when you are not logged in your HTTPCS account:
  - → On **HTTPCS Security**
    - **Start and end** of your security audit
    - **New** flaws detected
    - **Critical** flaws detected

Need classification (BANT approach Budget/Authority/Need/Timeline)

NEED

- ✓ What is your level of knowledge in cybersecurity?
- ✓ Have you already suffered from a cyber-attack?
- ✓ Have you defined your need?
- ✓ Do you perform security audits? How often? Are they manual or automated audits?
- ✓ Have you already implemented cybersecurity process?
- ✓ Do you already use any automated solutions to help you secure your website?
- ✓ Do you already use a web vulnerability scanner? If so, which one?
- ✓ How do you manage the zero false positives with it?
- ✓ Do you think this tool makes your team save a significant time or could it be improved?
- ✓ How many websites do you own?

BUDGET

- ✓ Do you have a specific budget for cybersecurity?

AUTHORITY

- ✓ Are you in charge of these issues?
- ✓ Do you have an IT team?
- ✓ How are you organized?
- ✓ Do you manage your security internally or is it outsourced?
- ✓ Do you correct the vulnerabilities internally?

TIMELINE

- ✓ When was your last audit and have you already planned the next one?

Some useful facts according to the needs and expectations you have identified

- **Your contact does not use any automated cybersecurity solutions yet or does not have any technical expertise:**
  Make him understand that SECURITY will allow him **to secure his website** easily / that it is easy to use, that once it is configured, it **runs automatically** and that he will receive all the information in the clearest way to correct his vulnerabilities easily.
- **Your contact uses only defensive security solutions (firewall, antivirus):**
  Make him understand the SECURITY's approach is different, that the defensive solutions are important but **are not enough against hacking** attacks.
- **Your contact has an internal team to correct the flaws:**
  Inform him he can **email the details** of each flaw to the person in charge of correcting it, that the simulation tool allows him to **redo the attack and to check it has been properly corrected**. Plus, a user right management option (SuperAdmin console) allows him to create and manage different user rights.
- **Your contact owns an / several ecommerce website(s):**
  Ask him what the **turnover / day** of the site is and to consider the **financial loss** of a hacking attack.

RECAP OF OUR 4 SOLUTIONS
PACK FULL

SECURITY

Zero-false-positive guaranteed applicative and web vulnerability scanner

Detects the vulnerabilities of a website or a web application, 365/year. Generates the **list of all the flaws** and the c**ountermeasures to apply**. The detailed **reports** allow to stay secure and to prevent from attacks easily. Once the corrections are applied, the HTTPCS certification **seal** is displayed on the user's website.

+

CYBER VIGILANCE

Real-time watch over the Dark net, the Deep web and the Web

Nowadays, all the companies may be a **target for hackers**. To adopt a "cyber vigilant" attitude is to implement a **proactive watch over the dark net** and the Internet!

HTTPCS Cyber Vigilance sends a **notification** whenever a sign of an underway attack is detected. Allows to be notified in real time before being the victim of a hacking attack or a data leak.

+

INTEGRITY

Monitoring from 50 censors worldwide of web availability and accessibility

HTTPCS Monitoring sends a notification whenever your **website is unavailable**. This "web ping" solution requests the server and the website every 60 seconds.

The user may add a **proof of integrity** to test also the accessibility of the website.

+

MONITORING

Continuous monitoring of fraudulent changes on a website and external sources

Allows to **keep control over the content** and **external sources** (scripts, tracking, advertising agency...) but also to follow the errors and **malicious files detection**.

HTTPCS Integrity sends immediately a text message or email notification whenever there is the **slightest change**. The solution to react **as quickly as possible**, before it is too late.

PACK FULL - 4 SOLUTIONS

- ✓ Unlimited number of audits
- ✓ Grey box audits
- ✓ Advanced audit configuration
- ✓ Complete results
- ✓ Free technical support 24/7