HOLM SECURITY

Web Application Scanning

Automated and continuous web application vulnerability assessment

Web Application Scanning

Several independent experts estimate that about 70% of all web applications i.e. websites, can be hacked. Gartner states that 75% of the attacks occur in the application layer, which makes web applications the most vulnerable layer in your IT environment. The fact that web applications are often exposed to the entire Internet dramatically increases the risk of vulnerabilities being exploited by malicious people.

Automatically and continuously

Our Web Appplication Scanning automatically and continuously scans your web apps and RESP APIs for an ever-increasing number of vulnerabilities. The scanning detects vulnerabilities related to flawed code, misconfigured systems, weak passwords and exposed system information, personal data and code.

Provided with out smart and effective tools , support service and comprehensive information, you or your IT partner can effectively prioritize and rectify detected vulnerabilities before they are exploited by a malicious person.

In parallel with a scheduled scanning of your web apps and systems, you can scan on demand at any time, for example in connection with changes and commissioning.

Covering the entire IT environment

Our scanners scan your public web apps, accessible via the Internet. By installing one or more Scanner Appliances in your local environments, behind your firewalls, we can scan all your public web apps – even if your IT environment is present in several physical locations. The data collected by our Scanner Appliances is presented in our control panel Security Center.

Vulnerability manager

Vulnerability Manager is a powerful tool for you to work effectively with vulnerabilities, regardless of whether you have a small number or thousands of vulnerabilites . You sort, group, ignore and prioritize the vulnerabilities in just the way that works best for you with the tool. The tool provides a range of functions for collaboration within your organization and with external partners, such as your IT partner.

Scan details

- ✓ Scans for a large number of general vulnerabilities
- ✓ Scans for several thousands of vulnerabilities in specific CMSs such as WordPress
- ✓ Scans for OWASP Top 10 vulnerabilities (version 2017)
- ✓ Detects vulnerabilities in REST APIs
- ✓ Supports scanning of local cloud infrastructure, such as AWS
- ✓ Detects web application configuration and rights errors
- ✓ Detects the exposure of personal data, system information, credit card numbers and passwords
- ✓ Fuzz testing— detects if a web application behaves irrationally or unexpectedly
- ✓ Scanning of web applications requiring authentication
- ✓ Warns if SSL certificates have expired, are about to expire or are unsafe
- ✓ Automatically identifies web servers, programming languages and databases
- ✓ Authenticated scan
- ✓ Automatic update of vulnerability database
- ✓ High precision with a low amount of false-positives

Other details

- ✓ No software or hardware requirements
- ✓ Automated and scheduled scans, as well as scans on demand
- ✓ Automated and manual structuring and grouping of devices
- ✓ Vulnerability Manager – administration of vulnerabilities
- ✓ Continuous Monitoring – monitoring of vulnerabilities and changes
- ✓ Functions for GDPR and NIS compliance
- ✓ Customizable detail and statistical reports
- ✓ Customizable dashboard for quick overview
- ✓ Full IPv6 support
- ✓ Administration via Security Center

Continuous Monitoring

The tool Continuous Monitoring allows you to quickly and easily structure the monitoring of changes that generates notifications and alarms. This tool removes the need to work in Security Center. Instead, you will be notified when new vulnerabilities are detected, when any changes are made and when vulnerabilities have been rectified. You can easily pinpoint, for example, web apps handling personal data for GDPR compliance.

Remediation

The service includes a complete tool for Remediation. The flow is largely automated. You set up rules for when to create cases and how to assign them. The tool supports integration with external remediation systems.

Reports

This service comes with ready-made templates, and the option to create your own reports – adaptable for both technicians and IT-specialists, as well as management and the board. The reports can be distributed in encrypted form to, for example, your IT partner or system vendor. Reports can be created on demand at any time or automatically according to your desired shedule.

Functions for GDPR and NIS compliance

The service offers a range of GDPR and NIS compliance support functions. You can, among other things, pinpoint web apps that handle personal data to monitor these and automatically generate continuous reports to the data controller.

Market-leading vulnerability assessments

Holm Security is a challenger in automated and continuous vulnerability assessments.

Our Holm Security VMP platform offers the ability for everyone to effectively take control of the security of their web apps, networks and systems. But we also offer innovative solutions to assess how secure your users are. Our platform is easy to use and you get extensive support from our support staff and security experts. An investment in our platform is, in short, a smart and efficient investment in increased security – not least when faced with a future where cyber security is becoming increasingly important to meet an increasing number of threats, new and existing laws and recommendations.

Contact

Holm Security
Gustavslundsvägen 141
SE-167 51 Bromma
Sweden
Telephone: +46 8-550 05 570
info@holmsecurity.com
www.holmsecurity.com