RISKIQ®

Securing Your Digital Footprint

Understanding website and web server security exposures

RiskIQ Digital Footprint® provides organizations with visibility into internet-facing assets that exist outside the security of your firewall. These assets are often critical to your organization, providing a way for your customers, prospects, and employees to interact through web sites, forms, web applications, and more.

Using RiskIQ's broad coverage of internet and threat data, Digital Footprint has the unique capability to quickly find and monitor web site and web server asset security from a deep, component level. This depth allows security teams to quickly locate specific assets which are running a particular version of a framework or web component, or to identify web sites that are not compliant with security policies.

OWASP Security Policies

Security teams can evaluate websites in their inventory based on the Open Web Application Security Project (OWASP) guidelines for secure websites.

During continuous scanning of the internet and websites, RiskIQ gathers details about website assets from their HTTP header response and the page content. This allows security teams to filter assets based on OWASP Secure Header security policies.

These security policies include:

- HTTP Strict Transport Security (HSTS)
- Public Key Pinning Extension for HTTP (HPKP)
- X-Frame-Options
- X-XSS-Protection
- X-Content-Type-Options

Websites which violate these security policies leave the server and visitors of those websites exposed to compromise and data theft.

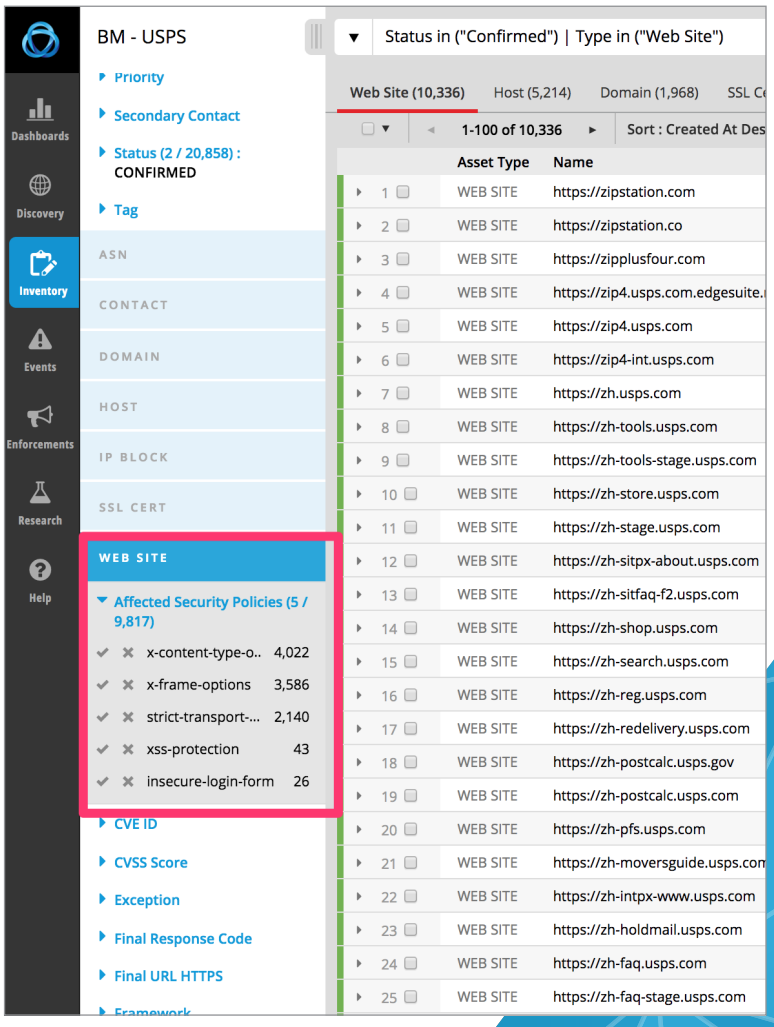

Fig 1. Filter assets based on OWASP security policy violation

Quickly Find Assets Affected by CVEs

Along with component-level detailing of assets, Digital Footprint also correlates known CVEs with those components. This provides organizations with the ability to quickly identify internet-exposed assets that may present a greater risk due to new or existing vulnerabilities.

- Detailing of assets and components includes:
- Web Component Type (Searchable)
- Web Component Name (Searchable)
- Web Component Version (Searchable)
- CVE ID (Searchable)
- CVSS Score (Searchable)
- First Seen
- Last Seen

The history of the components on assets provides details regarding the period of time in which a component of a particular version was seen active. This is helpful to determine when an asset may have been vulnerable to exploit.

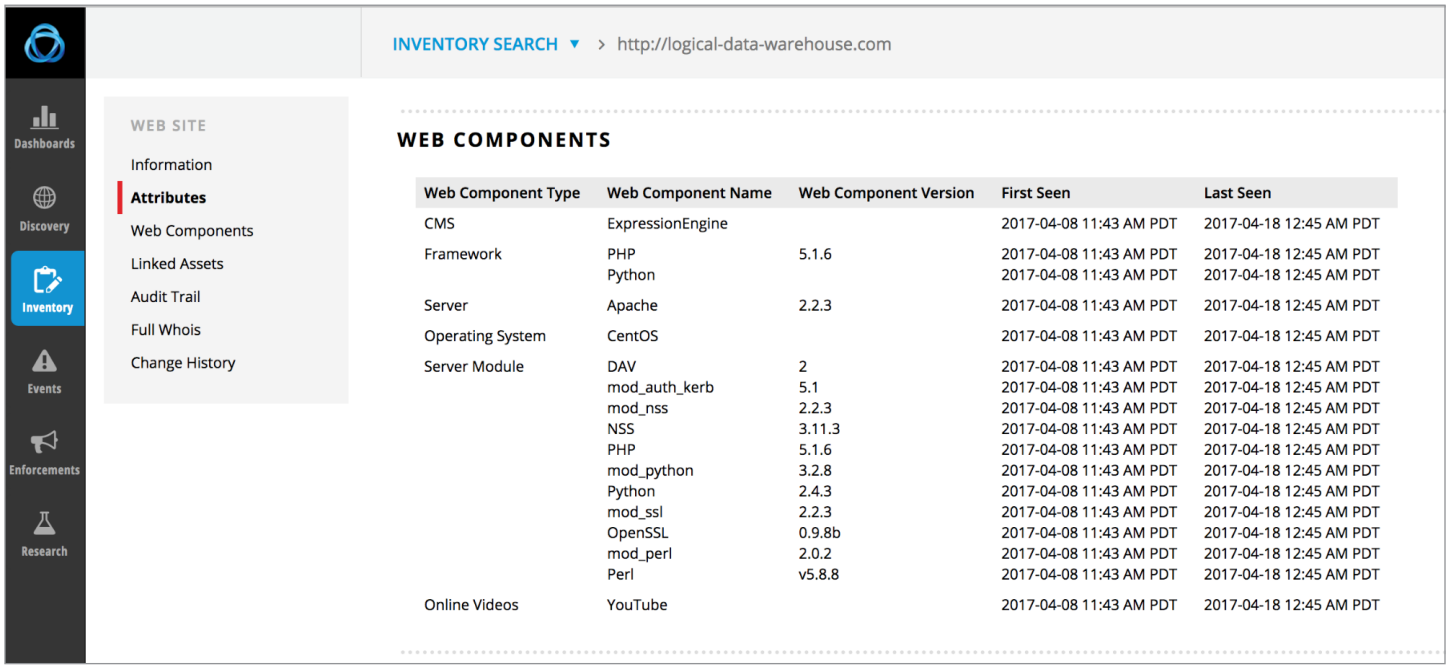

Fig 2. Example of a website with a rich set of components

RISKIQ®

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com