

Securing your Digital Footprint

Understanding website and web server security exposures



RiskIQ® Digital Footprint provides organizations with visibility into all 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 every website 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.

The screenshot displays the RiskIQ Digital Footprint interface. On the left is a navigation sidebar with icons for Dashboards, Discovery, Inventory, Events, Enforcements, Research, and Help. The main content area is titled 'BM - USPS' and shows a list of assets. A red box highlights the 'WEB SITE' section, which lists 'Affected Security Policies (5 / 9,817)'. The policies and their counts are:

Policy	Count
✓ x-content-type-o...	4,022
✓ x-frame-options	3,586
✓ strict-transport...	2,140
✗ xss-protection	43
✗ insecure-login-form	26

Below this list, there are links for 'CVE ID', 'CVSS Score', 'Exception', 'Final Response Code', 'Final URL HTTPS', and 'Framework'. On the right, a table shows a list of web sites, filtered by 'Status in ("Confirmed")' and 'Type in ("Web Site")'. The table has columns for 'Web Site (10,336)', 'Host (5,214)', 'Domain (1,968)', and 'SSL Ce'. The table is sorted by 'Created At Des' and shows a list of 25 items, each with a checkbox, a number, and a URL.

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.

Dashboards

Discovery

Inventory

Events

Enforcements

Research

INVENTORY SEARCH ▾ > http://logical-data-warehouse.com

WEB SITE

Information

Attributes

Web Components

Linked Assets

Audit Trail

Full Whois

Change History

WEB COMPONENTS

Web Component Type	Web Component Name	Web Component Version	First Seen	Last Seen
CMS	ExpressionEngine		2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
Framework	PHP	5.1.6	2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
	Python		2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
Server	Apache	2.2.3	2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
Operating System	CentOS		2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
Server Module	DAV	2	2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
	mod_auth_kerb	5.1	2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
	mod_nss	2.2.3	2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
	NSS	3.11.3	2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
	PHP	5.1.6	2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
	mod_python	3.2.8	2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
	Python	2.4.3	2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
	mod_ssl	2.2.3	2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
	OpenSSL	0.9.8b	2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
	mod_perl	2.0.2	2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
	Perl	v5.8.8	2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT
Online Videos	YouTube		2017-04-08 11:43 AM PDT	2017-04-18 12:45 AM PDT

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