

Assignment 5.1: Static Analysis of a Website (Secure Design)

Joshua A. Wortz

University of San Diego

CSOL-560

Dr Varma

11/03/2025

Overall analysis and score for	https://isc2.org
Score	<p>71 (SEO SCORE) 42 (PASSED) 8 (WARNINGS) - Configurations that are not strictly "broken" but represent a deviation from best practice. In cybersecurity, these are often risk acceptance decisions, for example, allowing heavy JavaScript for functionality at the cost of auditability. 11 (FAILED) - Clear deviations from standards. While SEO scanners flag these for "ranking," we view them as availability risks (slow load times) or client-side vulnerabilities (unsafe cross-origin links). 0 (UNRESOLVED) - Tests the scanner could not complete. In a security context, a high number of "unresolved" items is often a positive sign, indicating that a Web Application Firewall (WAF) is successfully blocking automated reconnaissance probes.</p>
Score based on	https://toolbox.seositecheckup.com/apps/general_analysis
Pros	<ul style="list-style-type: none"> ● Identity Assurance: The site correctly implements SPF records. This is critical for preventing domain spoofing and email phishing campaigns using the ISC2 brand. ● Strict Encryption: HTTPS is enforced with a valid certificate chain (DigiCert EV RSA) , ensuring data in transit is protected against Man-in-the-Middle (MitM) attacks. ● Reconnaissance Defense: The robots.txt file includes Disallow directives, preventing search engines from indexing sensitive internal directories or administrative portals. ● Canonicalization: The site correctly manages URL canonicalization, preventing "duplicate content" issues that can confuse security log analysis.
Cons	<ul style="list-style-type: none"> ● Client-Side Vulnerability (Reverse Tabnabbing): The scan detected target="_blank" links without rel="noopener". This is a security flaw where a malicious linked page can seize control of the ISC2 parent tab, potentially redirecting users to a phishing page. ● Availability Risk: The site load time is 6.72 seconds, significantly slower than the 5-second average. In a DDoS scenario, this heavy resource load makes the site easier to topple. ● Bloated Attack Surface: The DOM size (723 nodes)

	and heavy JavaScript execution (>3.5s) indicate a complex client-side architecture that is harder to audit for Cross-Site Scripting (XSS) flaws.
The title of page: Most search engines will truncate titles to 70 characters.	Length of 60 characters.
The meta description of page: The meta description tag is meant to be a short and accurate summary of page content. This description can affect search engine rankings and can also show up directly in search engine results (and affect whether or not the user clicks through to the site).	This webpage uses a meta description tag with a length of 236 characters. We recommend using well-written, inviting meta descriptions with a length of 150-220 characters (spaces included).
Robots.txt Test: Search engines send out tiny programs called spiders or robots to search your site and bring information back so that your pages can be indexed in the search results and found by web users. If there are files and directories you do not want indexed by search engines, you can use the "robots.txt" file to define where the robots should not go. These files are very simple text files that are placed on the root folder of your website. There are two important considerations when using "robots.txt": first, the "robots.txt" file is a publicly available file, so anyone can see what sections of your server you don't want robots to use; second, robots can ignore your "robots.txt", especially malware robots that scan the web for security vulnerabilities.	Site use a "robots.txt" file: https://www.isc2.org/robots.txt
Sitemap Test: This test checks	Found 1 sitemap file for the website:

<p>if the website is using a "sitemap" file: sitemap.xml, sitemap.xml.gz or sitemapindex.xml. Sitemaps are an easy way for webmasters to inform search engines about pages on their sites that are available for crawling. In its simplest form, a sitemap is an XML file that lists URLs for a site along with additional metadata about each URL (when it was last updated, how often it usually changes, and how important it is, relative to other URLs in the site) so that search engines can more intelligently crawl the site.</p>	<p>https://www.isc2.org/sitemap.xml</p>
<p>Favicon Test and Validator: Checks if site is using and correctly implementing a favicon. Favicons are small icons that appear in browser's URL navigation bar. They are also saved next to URL's title when bookmarking that page. They can help brand the site and make it easy for users to navigate to site among a list of bookmarks.</p>	<p>The site does have a favicon</p>
<p>Page Objects</p>	<p>Total objects: 113; Html pages: 5; Images: 36; CSS files: 4; Scripts: 35; CSS images: 0; Video files: 0;</p> <p>Page has more than 20 http requests, which can slow down page loading.</p>
<p>Code To Text Ratio: Checks webpage source code in order to measure the size of text content compared to the structure (HTML code). This percent is not a direct ranking factor for search engines but there are other factors that</p>	<p>Page size (source code) is 249 KB and content text size is 3 KB. Content text represents 1% from webpage source code. This is a low ratio and you might need to add more content!</p>

depend on it such as site loading speed and user experience.	
Google Analytics Test: Checks if website is connected with google analytics.	Website is using the asynchronous version of Google Analytics tracking code.
Google Preview: To see how webpage might look into a Google search results page. A Google search result uses webpage title, url and meta-description in order to display the information. If these elements are too long, Google will truncate their content.	https://www.isc2.org/Cybersecurity Certifications and Continuing Education ISC2ISC2 is the world's leading member association for cybersecurity professionals. Our members, candidates and associates are leading the cybersecurity
Keywords Cloud: The Keyword Cloud is a visual representation of keywords used on website. This will show which words are frequently used in the content of webpage.	<p>able accept added advance ahead allow</p> <p>browser building career cart center certificates</p> <p>certification certifications certified</p> <p>checkbox cissp community connect consent contact</p> <p>content continuing cookie cookies courses</p> <p>cyber cybersecurity date</p> <p>development device directly education enable</p> <p>enterprise event events exam experience free</p> <p>have help impact information insights</p> <p>interested journey just know label leadership</p> <p>learn learning links location london media mind</p> <p>november online pages partners peace</p> <p>performance preferences premier privacy</p> <p>professional protection provide pursuing reject risk</p> <p>schedule secure security services settings</p> <p>share site skills social software sscp start stay</p> <p>store strengthen team time topics training</p> <p>types used usually virtual visit website work world</p>
Page Cache Test: Checks if	The site correctly uses caching headers for JavaScript and CSS

<p>the site is serving cached pages. Caches reduce server-load (since pages are generated less often) and speeds up page display (by caching page output vs compiling the php-page). Caches also reduces bandwidth requirements by up to 80%. Caching makes most sense for high traffic pages whose content does not change on every page view. Common caching methods are Quickcache and jpcache.</p>	<p>resources. This improves availability by reducing server load during high-traffic periods.</p>
<p>Image Expires Tag Test: Checks if page is using an image expires tag, which specifies a future expiration date for images. Browsers will see this tag and caches the image in the user's browser until the specified date (so that it does not keep re-fetching the unchanged image from your server). This speeds up site the next time that user visits the site and requires the same image.</p>	<p>Passed. The webpage utilizes 'Expires' or 'Cache-Control' headers, allowing browsers to cache images locally. This reduces bandwidth consumption and server load for returning visitors.</p>
<p>URL Canonicalization Test: Test the site for potential URL canonicalization issues. Canonicalization describes how a site can use slightly different URLs for the same page (for example, if http://www.example.com and http://example.com displays the same page but do not resolve to the same URL). If this happens, search engines may be unsure as to which URL is the correct one to index.</p>	<p>https://www.isc2.org/ and https://isc2.org/ resolve to the same URL.</p>
<p>Directory Browsing Test:</p>	<p>The server has disabled directory browsing.</p>

Checks if server allows directory browsing. If directory browsing is disabled, visitors will not be able to browse the directory by accessing the directory directly (if there is no index.html file). This will protect files from being exposed to the public. Apache web server allows directory browsing by default. Disabling directory browsing is generally a good idea from a security standpoint.	
Libwww-perl Access Test: Botnet scripts that automatically look for vulnerabilities in the software are sometimes identified as User-Agent libwww-perl. By blocking access from libwww-perl you can eliminate many simpler attacks.	Test not included in this report version.
Server Signature Test: Checks if server signature is on. Turning off server signature is generally a good idea from a security standpoint.	Test not included in this report version.
Plaintext Emails Test: Checks webpage for plaintext email addresses. Any e-mail address posted in public is likely to be automatically collected by computer software used by bulk e-mailers (a process known as e-mail address harvesting). A spam harvester can read through the pages in the site and extract email addresses which are then added to bulk marketing databases and the result is more spam in the inbox.	Webpage does not include email addresses in plaintext
IP Canonicalization Test: Test	Test not included in this specific scan report.

the site for potential IP canonicalization issues. Canonicalization describes how a site can use slightly different URLs for the same page (for example, if the site's IP address and domain name display the same page but do not resolve to the same URL). If this happens, search engines may be unsure as to which URL is the correct one to index.	
Safe Browsing Test: Checks if website is listed with malware or phishing activity.	This site is not currently listed as suspicious (no malware or phishing activity found).
Social Media Check: Test if the website connects to at least one of the most important social networks.	Passed. The site includes Open Graph and Twitter Card meta tags, allowing for rich integration when content is shared on social platforms.
Social Media Activity: Checks the activity on social media networks of the website or URL. This activity is measured in total number of shares, likes, comments, tweets, plusOnes and pins and this activity covers only the URL and not social media accounts linked with the webpage.	This test wasn't in the report.
Most Common Keywords Test	The most common keywords are cookies 28, cybersecurity 14, site 11, certification 10, and security 10.
URL SEO Friendly Test	Passed. The URLs observed in the report (e.g., /Cybersecurity-Certifications) are semantic and readable. They rely on keywords rather than obscure database parameters (like ?id=552), which aids in both SEO and log analysis for security teams.
Underscores in Links Test	Passed. The site utilizes hyphens rather than underscores in its URL structure (e.g., isc2.org/robots.txt), which is the preferred standard for readability and search engine indexing.
Image Alt Test	This webpage uses "img" tags with empty or missing "alt" attributes! This is necessary for ADA compliance for screen

	readers, as well as for context with SEO optimization
Inline CSS Test	Passed. The report confirms that CSS resources are minified and cached. While some "Render Blocking" resources were found, the primary stylesheets are externalized, which allows for cleaner Content Security Policy (CSP) implementation.
Deprecated HTML Tags	This website does not use deprecated HTML tags
Nested Tables Test	Passed. The site utilizes modern HTML5 <div> structures (e.g., <div id="onetrust-banner-sdk">) rather than legacy nested tables. This reduces DOM complexity and prevents layout rendering issues on modern browsers.
JS Minification Test	All JavaScript files used by this webpage are minified
CSS Minification Test	All CSS resources used by this webpage are minified.
MOBILE USABILITY	Passed (100/100). The site is fully optimized for mobile viewports, ensuring that security controls (like cookie banners and login forms) remain accessible on smaller screens.
Media Query Responsive Test	Passed. The site correctly utilizes CSS media queries to adapt the layout for different device sizes, ensuring mobile usability.

References

International Information System Security Certification Consortium (ISC2). (n.d.).

Cybersecurity certifications and continuing education. <https://www.isc2.org>

SEO Site Checkup. (2025). *SEO analysis of isc2.org.* <https://seositecheckup.com>