

USER MANUAL

THREAT SCANNING

Threat Scanning

Threat Scanning is an easy-to-use website and firewall scanning solution designed to help businesses identify vulnerabilities that may be exploited in their websites and firewalls. With only a few quick steps, uRISQ will begin providing monthly or weekly scanning of your website and public firewall. Administrators and Threat Scanning users will be notified when scans are complete with a summary of potential vulnerabilities and if there have been any changes from the previous scan. This allows you to take swift action to remediate exposures and mitigate any compromise in sensitive data before it is too late.

Firewall Threat Scanning

Businesses that have internet connectivity in their office(s) have a router/firewall in place to manage traffic. Sometimes that router is provided by their Internet Service Provider and sometimes an additional managed router is put into place to provide additional monitoring and management. Regardless the case, the publicly router/firewall has “virtual doors”, call ports, that can be used to access a network.

Threat Scanning, scans 911 ports and provides a report of risks associated with open ports that were found.

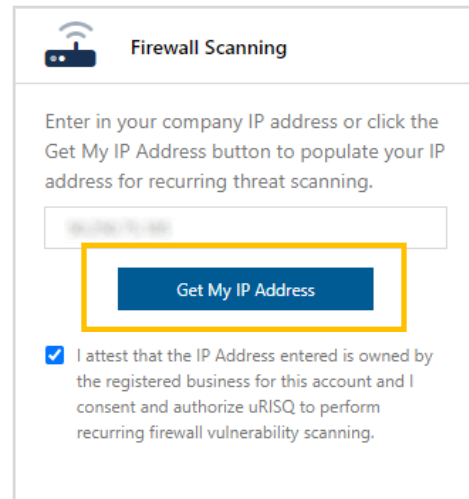
Adding your IP address

While adding your IP address may seem like a daunting task, uRISQ has made it simple by providing a button that will populate your IP address for you (if you are currently connected to the network, you want scanned).

Single IP Scanning Configuration

During the registration process, uRISQ prompts you to configure your threat scanning settings. You can always make modifications to your settings by going into the Threat Scanning Settings and updating the IP address field. To set up or make changes to your settings:

1. Go to Threat Scanning in the navigation and select Settings
2. Selecting the 'Get My IP Address' option will automatically populate the IP address of the network you are currently connected to. You may also manually enter the IP Address.
3. Check the checkbox attesting to ownership and authorization
4. Click the Save Scanning Settings button



The screenshot shows a web interface titled "Firewall Scanning" with a router icon. It contains a text input field for an IP address, a "Get My IP Address" button highlighted with a yellow box, and a checkbox with a blue checkmark. Below the checkbox is a paragraph of text: "I attest that the IP Address entered is owned by the registered business for this account and I consent and authorize uRISQ to perform recurring firewall vulnerability scanning."

Website Threat Scanning

uRISQ's website scanner is an automated website scanner that will scan for vulnerabilities within a public facing, web-based solutions, like a website. The uRISQ Website scanner spiders first crawl the entire application, analyzing, in-depth, each page to audit for security vulnerabilities. uRISQ checks for vulnerabilities on the web server, proxy server, web application server and other web services and ports.

Important facts of the uRISQ website scanner include:

- ability to analyze different web technologies, such as PHP, ASP.NET, ASP, etc.
- ability to scale to process large websites, if needed
- ability to produce readable and actionable results without requiring extensive web security know-how.

Threat Scanning Configuration

When you log in for the first time, you will be prompted with the Threat Scanning Settings panel. Adding your website and IP address is a straightforward process that only takes a few steps. If you choose to bypass Threat Scanning Settings, you can access your settings at any time by:

1. Click on Threat Scanning in the left side navigation
2. Click on Settings

If you want to skip the Threat Scanning setup and do not wish to see this form upon logging in in the future, simply select the 'No thanks, do not show this at start up' checkbox at the bottom of the panel.

Threat Scanning Settings

Why Vulnerability Scanning is Important

Understanding your vulnerabilities helps you understand your risk. uRISQ Threat Scanning provides insight into where your website or your firewall may be vulnerable. New vulnerabilities pop up all the time. Let uRISQ help you be aware of changes to your environments or new threats that can weaken your current safeguards.

Website Scanning

Enter in your company website for recurring threat scanning.

Enter in a valid website address. Invalid or improperly formatted website addresses may not pass our validation process and may cause problems with your scans.

☐ I attest that the website entered is owned by the registered business for this account and I consent and authorize uRISQ to perform recurring website vulnerability scanning.

Firewall Scanning

Enter in your company IP address or click the Get My IP Address button to populate your IP address for recurring threat scanning.

☐ I attest that the IP Address entered is owned by the registered business for this account and I consent and authorize uRISQ to perform recurring firewall vulnerability scanning.

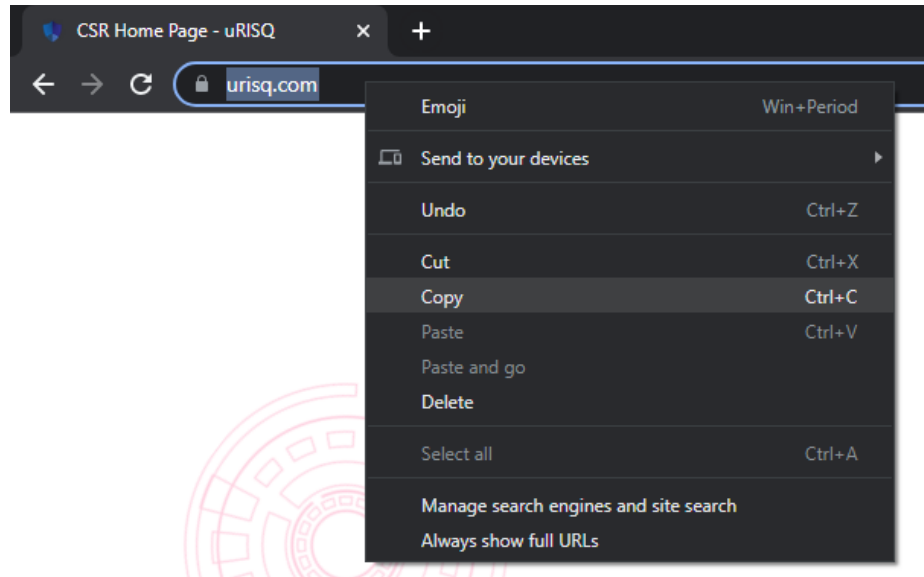
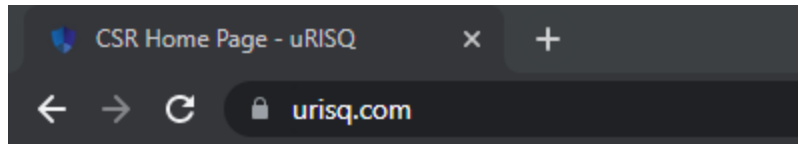
☐ No thanks, do not show this at start up.


Adding Your Website

Adding your website address is an easy process but it is important to ensure to enter in the full address. An example of a properly formatted website address would be '**https://urisq.com**'. The address begins with '**https://**' and ends with '**.com**', '**.org**', '**.net**', etc.

The simplest way to ensure you enter your complete website address is to:

1. Launch your website in a browser
2. Click in the website address located in your address bar in your browser so it is highlighted
3. Copy the address (Ctrl+C)
4. Paste it into the website field on the Settings page (Ctrl+V)
5. Check the checkbox attesting to ownership and authorization
6. Click Save Scanning Settings





Website Scanning

Enter in your company website for recurring threat scanning.

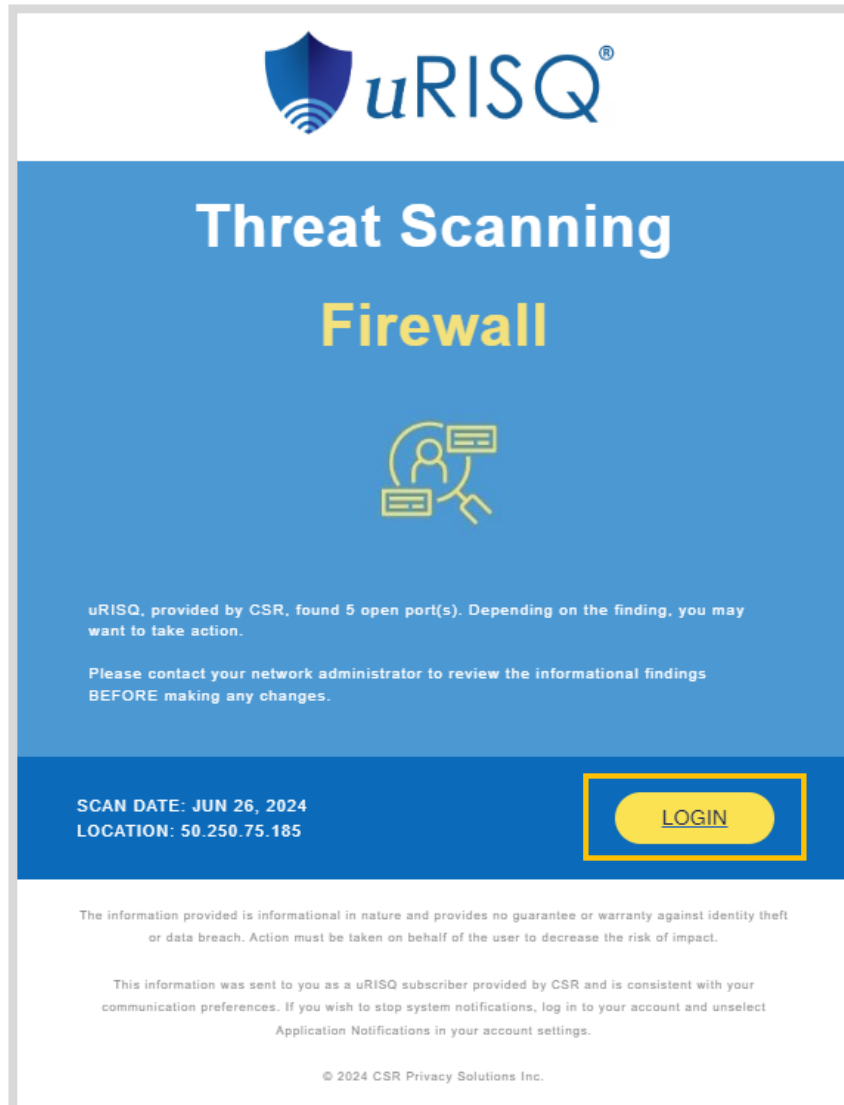
Enter in a valid website address. Invalid or improperly formatted website addresses may not pass our validation process and may cause problems with your scans.

☒ I attest that the website entered is owned by the registered business for this account and I consent and authorize uRISQ to perform recurring website vulnerability scanning.

Once you have completed filling in the desired sections and verified that the checkbox is filled for the appropriate sections, you may select 'Save Scanning Settings' to begin receiving your weekly or monthly reports.

Reporting

Once Threat Scanning configuration is completed, your scans will be queued into the uRISQ scanning engines. Once your scan is completed, you will receive an email notifying of completion and a summary of the scan. To view the details of the report, click the Login button in the email.



Accessing Reports

There are two ways to access your reports:

1. Clicking the Login button from your scanning completed email
2. Logging directly into uRISQ

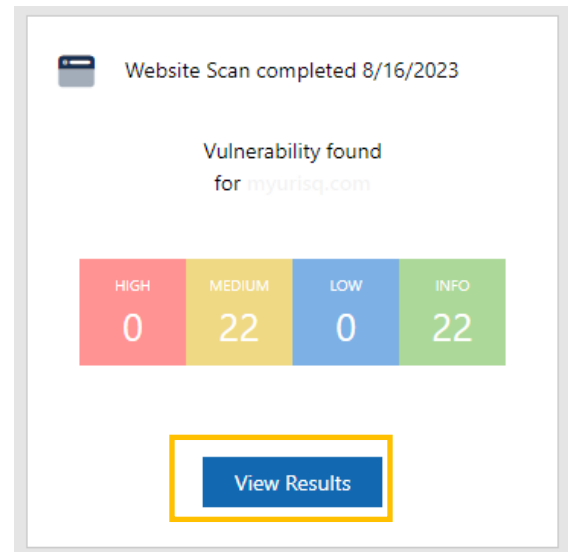
The email will provide a results summary such as:

- The date of completion
- If there are any changes from the previous scan
- The website address scanned
- The total number of vulnerabilities found previously

Click the LOGIN button to directly access the respective report.

To access the reports directly:

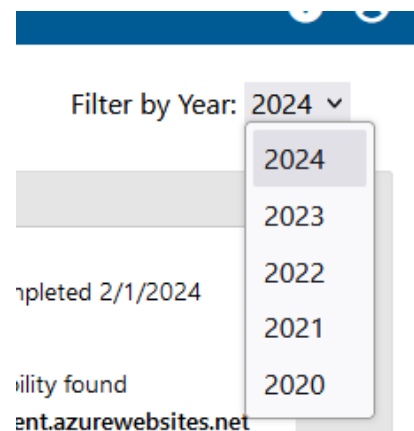
1. Log into uRISQ at <https://urisq.net>
2. Click on Threat Scanning
3. The Reports page will display
4. Website Scan Results will be displayed to the left
5. Each scan will have a line item
6. Click on the View Results on scan you wish to view



Filtering Reports by Year

The main report page is filtered by year to make finding results easier. Look to the far right to select the year you wish to view.

The reporting page will always load with the current year's results. To view historical scan, use the dropdown and select the year you wish to view.

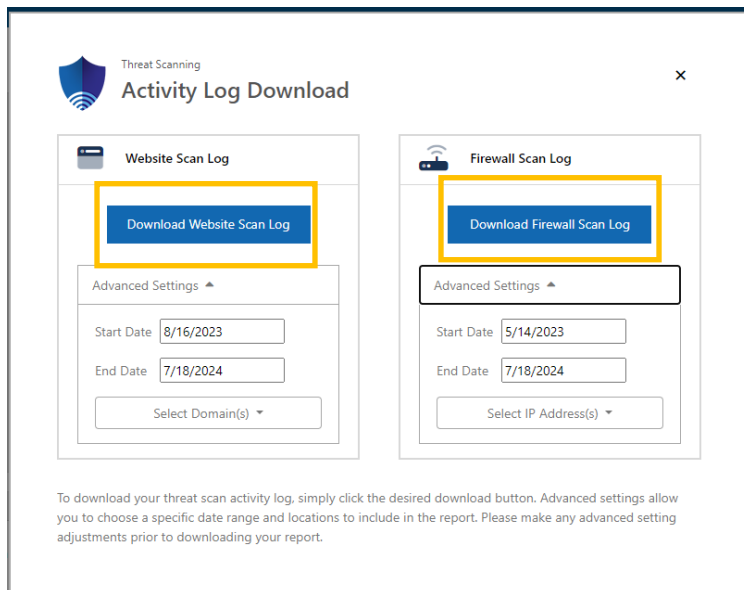
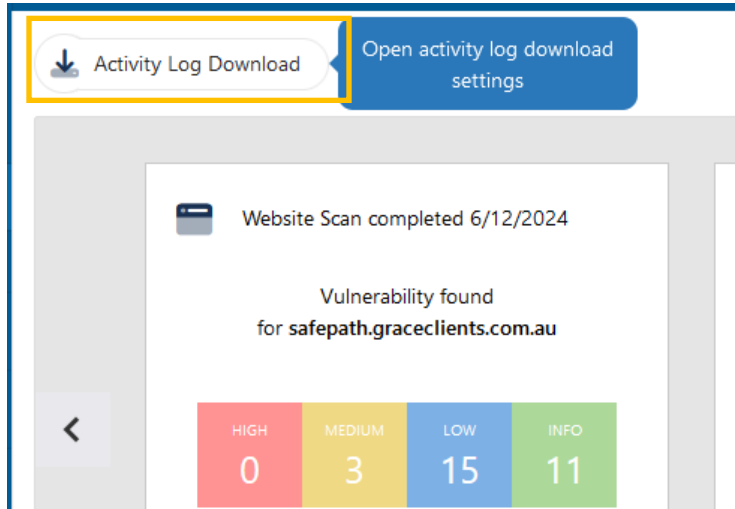


Reports Activity Log Download

uRISQ provides the ability to add activity notes to each scan report. Activity Logs provide businesses with proof of compliance. The Activity Log Download makes accessing multiple logs easier. The download feature allows authorized users the ability to download logs of multiple website reports or multiple firewall reports into one file. To download Threat Scanning Activity Logs:

1. Go to Threat Scanning
2. On the top of the Reports page there is a download icon, when you hover over it, it expands, and you will see the Activity Log Download button.
3. Click on the Activity Log Download button
4. The Activity Log Download window will open
5. Select which type of log you want to download, Website or Firewall

6. You can also click on Advanced Settings and select a date range or specific domains or IP addresses. If you do not make any advanced setting changes a full report will be generated for the respective scan type, website or firewall.
7. Click on the respective Download scan log button

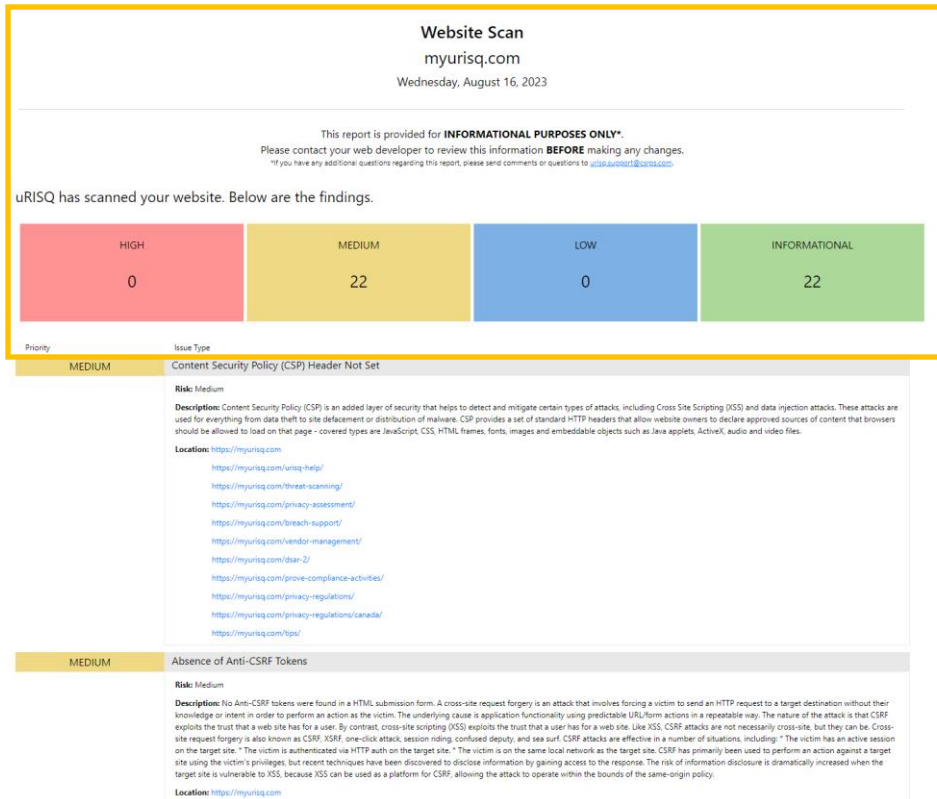


The activity report will download the activity log in a PDF document.

Understanding Your Website Scan Results

The website scan report will display a summary of the scan, to include:

1. Website scanned
2. Date Scanned
3. Categorized findings (High, Medium, Low and Informational)



The uRISQ categorizes are based on industry categories for the vulnerabilities found.

1. High should be reviewed and remediation should be prioritized. High priority vulnerabilities should be addressed and present a high risk.
2. Medium should be reviewed, however some medium vulnerabilities are caused by business level decisions, such as implementing a third-party form on your website. Each vulnerability needs to be reviewed and determined if the business reason outweighs the risk.
3. Low should be reviewed but are lower in priority
4. Informational are vulnerabilities but are the lowest level of risk

It is always best practice to review all vulnerabilities at least once. Once you have reviewed the vulnerabilities it is highly recommended to [enter in a report note](#) into the respective report where the vulnerability was found.

Below the summary of findings are the details of each issue type which includes:

1. Priority/Risk Level
2. Description of the vulnerability found
3. Location(s) where vulnerability was found

Website Scan
myurisdq.com
Wednesday, August 16, 2023

This report is provided for **INFORMATIONAL PURPOSES ONLY**.
Please contact your web developer to review this information **BEFORE** making any changes.
*If you have any additional questions regarding this report, please send comments or questions to info@myurisdq.com

uRISQ has scanned your website. Below are the findings.

HIGH		MEDIUM		LOW		INFORMATIONAL	
0		22		0		22	
Priority	Issue Type						
MEDIUM	Content Security Policy (CSP) Header Not Set						
Risk: Medium							
Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page - covered types are JavaScript, CSS, HTML, frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.							
Location: https://myurisdq.com							
https://myurisdq.com/urisdq-help/							
https://myurisdq.com/threat-scanning/							
https://myurisdq.com/privacy-assessment/							
https://myurisdq.com/breach-support/							
https://myurisdq.com/vendor-management/							
https://myurisdq.com/dsan-2/							
https://myurisdq.com/prove-compliance-activities/							
https://myurisdq.com/privacy-regulations/							
https://myurisdq.com/privacy-regulations/kanada/							
https://myurisdq.com/tips/							
MEDIUM	Absence of Anti-CSRF Tokens						
Risk: Medium							
Description: No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: "The victim has an active session on the target site." "The victim is authenticated via HTTP auth on the target site." "The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.							
Location: https://myurisdq.com							

And below the findings detail is the OWASP Top 10 Results (<https://owasp.org>).

INFORMATIONAL

Information Disclosure - Suspicious Comments

OWASP Top 10

The worldwide non-profit organization Open Web Application Security Project (OWASP)'s list of the ten most common vulnerabilities, known as OWASP Top 10, is often used as a security standard.
Visit <https://owasp.org> for more information on OWASP Top 10

2017

2021

8/10

Good!

✗

A1. Broken Access Control

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

✓

A2. Cryptographic Failures

The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information, and business secrets require extra protection, mainly if that data falls under privacy laws, e.g., EU's General Data Protection Regulation (GDPR), or regulations, e.g., financial data protection such as PCI Data Security Standard (PCI DSS).

✓

A3. Injection

Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection. The concept is identical among all interpreters. Source code review is the best method of detecting if applications are vulnerable to injections. Automated testing of all parameters, headers, URL, cookies, JSON, SOAP, and XML data inputs is strongly encouraged. Organizations can include static (SAST), dynamic (DAST) and interactive (IAST) application security testing tools into the CI/CD pipeline to identify introduced injection flaws before production deployment.

✓

A4. Insecure Design

Insecure design is a broad category representing different weaknesses, expressed as "missing or ineffective control design." Insecure design is not the source for all other Top 10 risk categories. There is a difference between insecure design and insecure implementation. We differentiate between design flaws and implementation defects for a reason: they have different root causes and remediation. A secure design can still have implementation defects leading to vulnerabilities that may be exploited. An insecure design cannot be fixed by a perfect implementation as by definition, needed security controls were never created to defend against specific attacks. One of the factors that contribute to insecure design is the lack of business risk profiling inherent in the software or system being developed, and thus the failure to determine what level of security design is required.

✗

A5. Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

✓

A6. Vulnerable and Outdated Components

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

Report Notes

Each report has a report note section to the right side of the scan report. When review, remediation, or acceptance of a finding occurs, enter in a report note:

1. Open up the respective scan report
2. Go to the right column and type in your report. Each note cannot be over 500 characters. If you need to add more than 500 characters, break your note into multiple entries.
3. Click Save Note
4. The note will appear below the Note field and button
- 5.

Selecting 'View Results' will navigate you to the complete report for this website scan. Report notes are downloadable in the [Activity Log Download](#).

Report Notes:

ADD NOTE

Enter note text... (500 characters maximum)

Save Note

DATE: 7/10/2024

USER:
jheyms+demo@growingtechnologies.com

NOTE:
test

note

DATE: 5/2/2024

USER:
jheyms+demo@growingtechnologies.com

NOTE:
test

DATE: 4/26/2024

USER:
jheyms+demo@growingtechnologies.com

NOTE:
test

DATE: 3/20/2024

USER:
jheyms+demo@growingtechnologies.com

NOTE:
test

Understanding Your Firewall Scan Results

Like your website scans, you will be able to access your firewall scan report from the Threat Scanning Report page or from the threat scanning scan notification email.

The firewall Scan report displays a summary of the scan to include:

1. IP address scanned
2. Date Scanned
3. Categorization of findings (High Medium, Low, and Informational)

The first section summarizes the basic information of the scan performed. Here you will find the Firewall IP, the date of the scan, and the risk level and open port count associated with the scan results.

Firewall Scan

107.199.214.133

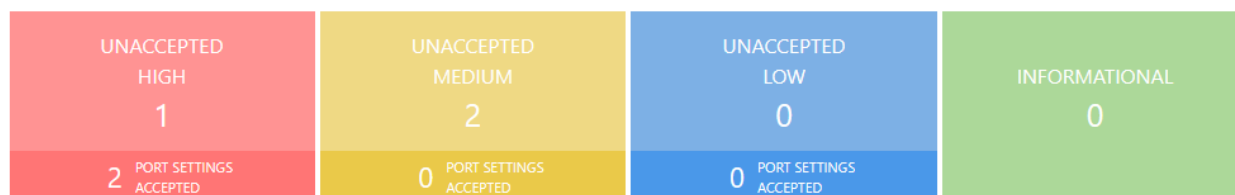
Wednesday, January 15, 2025

This report is provided for **INFORMATIONAL PURPOSES ONLY**.*

Please contact your administrator to review this information **BEFORE** making any changes.

*If you have any additional questions regarding this report, please send comments or questions to urisq.support@csrps.com.

uRISQ has scanned 911 ports. Below are the open ports.



The uRISQ categorizes are based on industry categories for the vulnerabilities found.

1. High should be reviewed and remediation should be prioritized. High priority vulnerabilities should be addressed and present a high risk.
2. Medium should be reviewed, however some medium vulnerabilities are caused by business level decisions, such as needing VPN access or opening a port for a specific server. Each vulnerability needs to be reviewed and determined if the business reason outweighs the risk.
3. Low should be reviewed but are lower in priority
4. Informational are vulnerabilities but are the lowest level of risk

It is always best practice to review all vulnerabilities at least once. Once you have reviewed the vulnerabilities it is highly recommended to [enter in a report note](#) into the respective report where the vulnerability was found.

Vulnerabilities found are listed below the categorization of vulnerabilities. Only ports that are open will be displayed. The firewall report will provide the following information:

1. Risk level of the port
2. Port number
3. Service commonly associated with the port and common vulnerabilities which may target that port

Port	Service	Accept Risk ^①
53	Domain Name Server (DNS) Common Vulnerabilities: Denial of Service, DNS Spoofing	<input checked="" type="checkbox"/> YES
3128	squid-https / ndl-aas Common Vulnerabilities: Denial of Service, Malware, Man-in-the Middle	<input checked="" type="checkbox"/> YES
8181	intermapper Common Vulnerabilities: Denial of Service, Malware, Man-in-the Middle	<input type="checkbox"/> NO
22	SSH Common Vulnerabilities: If required, implement additional controls such as multi-factor authentication and a VPN to encrypt traffic.	<input type="checkbox"/> NO
443	TSL/SSL Common Vulnerabilities: If required, implement additional controls such as an intrusion detection/prevention solution.	<input type="checkbox"/> NO

The final section is the [Report Notes](#) that offers you the ability to put any notes that may be pertinent for this report. These notes will be listed in descending order and include the date, user that added the note, and the note text.

Report Notes:

ADD NOTE

Enter note text... (500 characters maximum)



Save Note

DATE: 4/14/2022

USER: [Redacted]

NOTE: Gave to network engineer to close port 8181

1