Aura RedEye is an industry leading managed vulnerability scanning service. We assist customers in identifying security issues and vulnerability management.

Aura RedEye is not just another vulnerability scanner. Effectively managing large numbers of vulnerabilities across multiple networks, can be a challenging task. Our award winning service has evolved to ensure clients' issues are identified, managed, and resolved as quickly as possible.

Our scanning engines use best-of-breed open source and proprietary tools configured for your unique environment; Increasing the number and reliability of vulnerabilities identified while minimising false positives. Aura's security consultants analyse all scan results, interpreting your issues, applying context and evaluating the risk of the vulnerability to your organisation. RedEye notifications will alert you to issues, vulnerabilities or threats requiring your attention as soon as they are identified.

RedEye expedites vulnerability resolution by providing a direct communication path to Aura’s security consultants who are able to answer your questions or provide any additional information required.

RedEye's scanning frequency can be tuned to meet your organisations information security policy requirements, environment restrictions, or project timelines. Scans are typically run daily, weekly, monthly or as required after any major system or environment changes. This way you are notified and able react in a timely manner to new threats as they hit the Internet.

Web vulnerability scanning:

RedEye scans all websites and discoverable pages for web application security vulnerabilities. Web scanning includes (but is not limited to):

- OWASP top 10 vulnerabilities,
- Common weaknesses in each web technology E.G. PHP, .Net, java, etc.,
- Application logic weaknesses such as brute-forcing of credentials, bypassing of validation, etc.,
- Poor exception and error handling,
- Common technical feature flaws such as file-upload, dynamic report querying, site administration, etc.

Possible web scanning issues:

RedEye is designed and tuned to prevent disruption on production systems. RedEye performs a discovery scan to determine how your website behaves and reacts to web scanning and if further tuning and scan customisation is required. Discovery scans are best run outside of normal business hours to prevent any performance or user issues.

Web scanning should not adversely affect server load or application response times. Most web applications are able to be scanned with no noticeable service degradation.

Successful web scanning relies on a number of factors including:

- Compliance to common web standards,
- Available network bandwidth,
- Resources (memory and CPU) allocated to web server processes,
- WAF, IDS and IPS systems configured to permit requests from RedEye scanners.

RedEye is unable to pre-empt load on infrastructure or web applications due to variable network conditions, web application design, implementation and configuration.
Hosting providers with request logging enabled at the webserver level can provide and monitor the number of requests per second and resources consumed.

I'm a hosting provider and I have discovered an issue from a RedEye scan:

Before raising the issue with your client please confirm the issue is being caused by traffic from an Aura RedEye scanner. The IP addresses of all scanners can be requested from RedEye support. If required you can block the offending traffic at your border gateway device; if this is done please notify RedEye operations or support as soon as possible. It is important to ensure the asset owner or client is notified immediately to begin the resolution process. All subsequent scans will be reported as failed to the client until resolved.

It is also important to note other hosted assets may be affected should a complete block of all traffic be imposed. We recommend a granular approach to blocking requests to specific assets.

What can be done to help with problematic scans:

At Aura's discretion, assets suffering performance issues as a result of web scanning can be migrated to a scanner with request throttling. Throttled scans significantly reduces the rate of requests therefore lengthening the total scan time. As a result, throttled scans are run at most once a week.

Other considerations:

If required, RedEye can ensure all scans are executed from defined static IP addresses. An up to date list of IP addresses can be requested from RedEye support. Asset owners will be notified of any changes relating to scan schedules or traffic origins.

RedEye scan traffic may originate from one or more of the following IP Addresses:

210.4.209.57
203.97.154.129
202.174.114.88
202.174.114.111
202.174.114.112
103.7.168.135