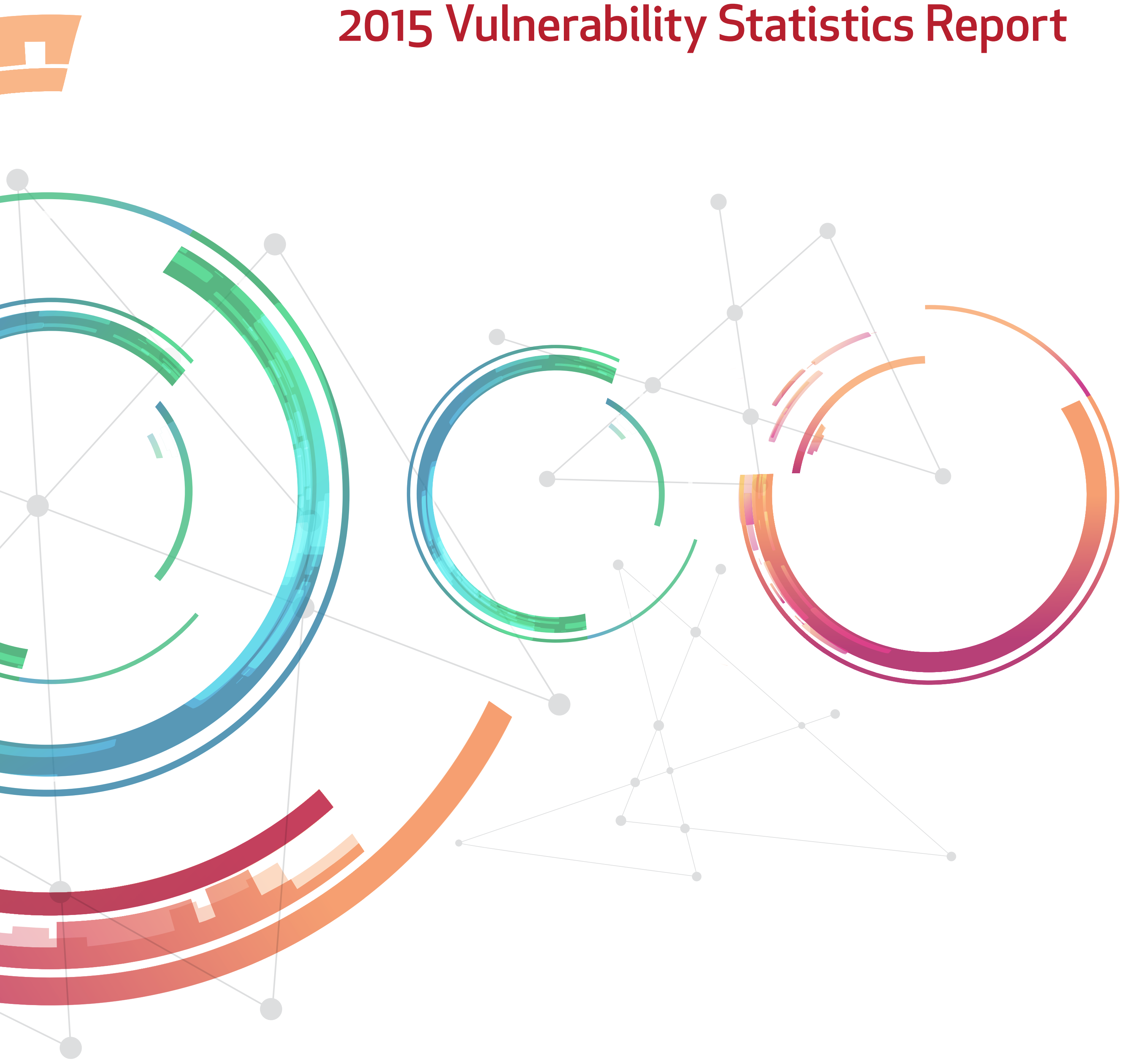
edgescan™

2015 Vulnerability Statistics Report



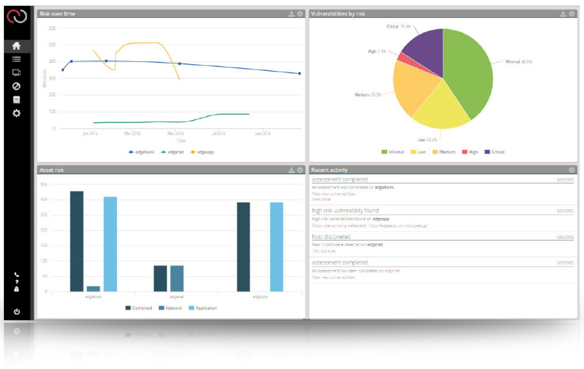
Introduction

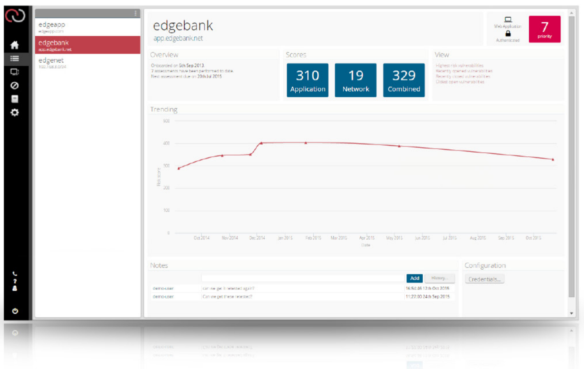
Vulnerabilities or bugs in software may enable cyber criminals to exploit both Internet facing and internal systems. Fraud, theft (financial, identity or data) and denial-of-service attacks are often the result, leaving companies with serious losses or damage of reputation. However, some of these issues can be easily avoided or at least mitigated.

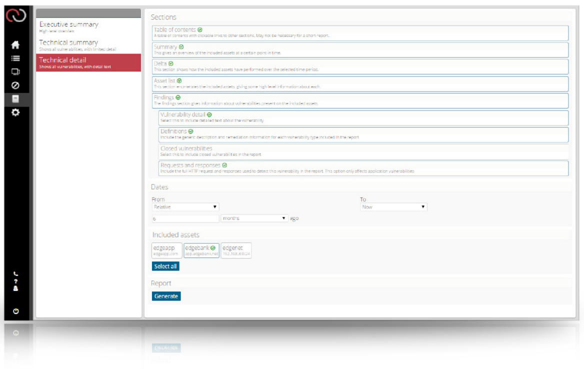
This document discusses the vulnerabilities discovered by **edgescan™** over the past year – 2015.

The vulnerabilities discovered are a result of providing continuous vulnerability management to a wide range of client verticals; from Small Businesses to Global Enterprises; Telecoms & Media, Software Development, Gaming, Energy and Medical organisations.

edgescan™ Portal







About edgescan™

SaaS: edgescan™ is a Software-as-a-Service (SaaS) vulnerability management service which provides continuous detection and validation of vulnerabilities in both web & mobile applications and hosting servers alike.

Accuracy: All vulnerabilities discovered by **edgescan™** are verified by our expert security analysts to make sure they are a real and appropriately risk rated. Our validated findings provide actionable intelligence and remediation advice to help you maintain a secure posture.

"Full-stack" Scalable Assessments: edgescan™ scales to hundreds or thousands of servers and web applications whilst still maintaining accuracy and coverage.

edgescan™ detects both known (CVE) vulnerabilities and also web application vulnerabilities unique to the application being assessed due to our hybrid assessment approach.

Analytics & Depth: Coupling leading-edge risk analytics, production-safe automation and human intelligence, **edgescan™** provides deep authenticated and unauthenticated vulnerability assessment across all layers of a systems technical stack.

Our **edgescan™** Advanced service also provides deep logical and behavioural testing on demand. Both Internal and public Internet facing systems can be assessed using **edgescan™**.

Integration & Alerting: edgescan™ provides integration via its API and JIRA plugin to easily integrate with other bug tracking and GRC systems. It also has customisable real-time alerting to inform you if a new vulnerability has been discovered.

Continuous Asset Profiling: edgescan™ provides continuous asset profiling, alerting you to changes in your environment and eliminate network blind spots via our unique HIDE (Host Index Detection & Enumeration) technology.

Gartner "SAMPLE VENDOR" Gartner Hype Cycle for Application Security 2015

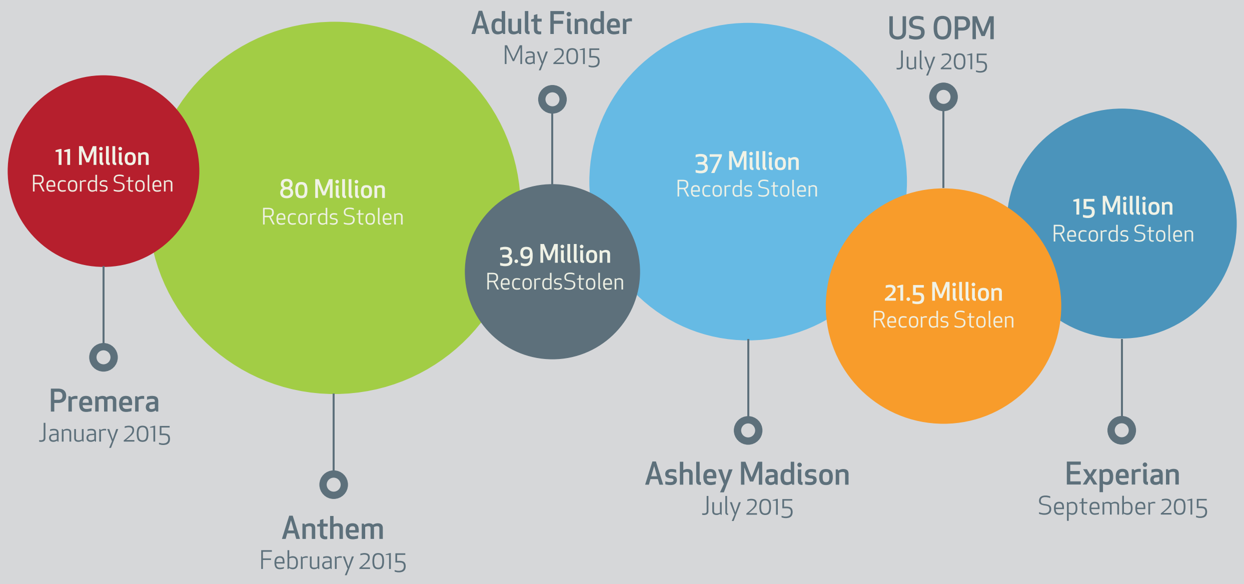
Gartner "NOTABLE VENDOR" Magic Quadrant for Managed Security Services

SME AWARDS FINALIST 2015

2015 Tech EXCELLENCE AWARDS

2015 in Review – Executive Summary

2015 has been a year of large security breaches:



The above are examples of significant system breaches resulting in millions of records and personal data being stolen.

Why?

Awareness, Detection and Response are key aspects in defending against cyber-attacks and **edgescan™** helps with this approach.

In terms of operational approaches, organisational trends towards DevSecOps should assist with security becoming more integrated and earlier in the system development lifecycle; "Pushing Left".

Hosting systems: Using Secure Baselines or Builds in cloud environments such that when vulnerabilities are discovered, rather than patch, we deploy a new baseline.

Error monitoring and log analysis solutions are also assisting with detective controls and helping organisations detect anomalies earlier and reacting quicker.

Overall host & server security below layer 7 is still a rich area for vulnerabilities.

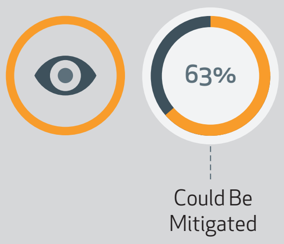
Application Layer: A drive towards DAST and SAST integration into the build process is catching issues "early and often" which assists in more secure software.

We still see "component security" being overlooked. Components can be defined as open source code, frameworks and code used by developers but not written by the application developer teams.

Component Security (Application Security Food-Chain)

Of all the vulnerabilities discovered by edgescan™ in 2015, 63% could have been mitigated via patch, configuration and component management combined.

Patching and component management relates to web applications, frameworks and hosting servers running insecure instances and services. In terms of web applications, many instances of insecure frameworks, plugins, components to support Cryptography, HTTP, language processors and parsers, contained exploitable vulnerabilities. In addition, the operating systems and services supporting such components also had known vulnerabilities (CVE's).



Our measuring tool and data repository

As discussed above, the vulnerability data used for this report has all been discovered on our clients systems over the past year (2015). All of the findings in edgescan are manually validated and risk rated to ensure accuracy and also to assist our clients with understanding which issues need to be prioritised.

Assets: edgescan assesses both server and web application layer systems for vulnerabilities. For our clients we call these collectively "Assets". This gives our clients the ability to group similar and related systems into asset groups for easier management.

15.1% of Assets have high or critical risk vulnerabilities

High or critical vulnerabilities are defined as:

- Easily exploitable
- Remotely exploitable
- Such issues can affect both application and network layers combined in some cases

Root Cause: Coding errors, Configuration flaws and out-of-date/No patching applied.

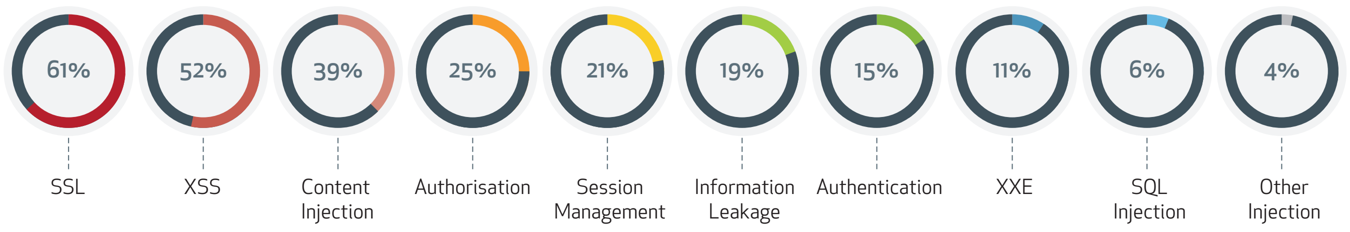
Remediation: Even though patch management is not as exciting as other aspects of security, it's still a vital aspect of maintaining a secure and robust posture. Security patches are a result of security bugs being discovered in application, framework & operating systems provided by system vendors.

In relation to web application security we still talk about Secure Application Development. It's our view that security touch points and developer education is a good starting place to correct the problem.

Vulnerability Statistics

Web Applications and Web Site Security:

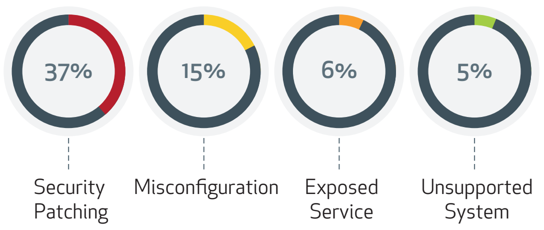
Likelihood of a vulnerability being discovered – Web Applications



Above is a snapshot of the most common vulnerabilities discovered in 2015 for the web application layer as discovered by **edgescan™**. As you can see, SSL/Crypto weaknesses are most common followed by Cross-Site-Scripting (XSS). SQL Injection is thankfully less common, akin to other injection vulnerabilities (Command Injection, Remote Code Execution), all of which can result in total system-wide compromise.

A new entry to the list is **XML eXternal Entity** attacks (XXE) which leverages XML parser misconfiguration and can result in data compromise.

Likelihood of a vulnerability being discovered in Hosting & Component Layers by root cause



In relation to hosting security, 37% of hosting layer vulnerabilities could have been prevented by adopting a robust approach to patching. Patching relates to keeping the hosting and component system up-to-date to help close-off known risks. Misconfiguration, Exposed Services and Unsupported Systems relate to both Operating systems and hosted frameworks or components.

Maintenance and component security are key to maintaining a robust approach to full-stack security.

edgescan™

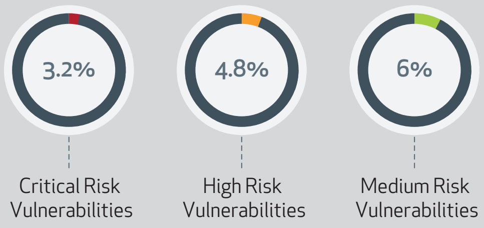
Risk Density

In 2015 we discovered on average 1.5 Critical, High or Medium risk vulnerabilities per asset assessed.

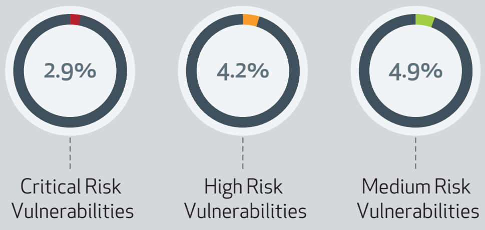
This is a result of insecure coding practices on the web layer, poor component / framework and operating system security weaknesses. The vulnerabilities ranged from remote code execution, to command Injection to SQL Injection.

Vulnerabilities like Shellshock, Poodle and Logjam were common across hosting environments. Apache, Adobe and Microsoft systems and services were the platforms with the highest risk density.

Risk Profile – Application Layer

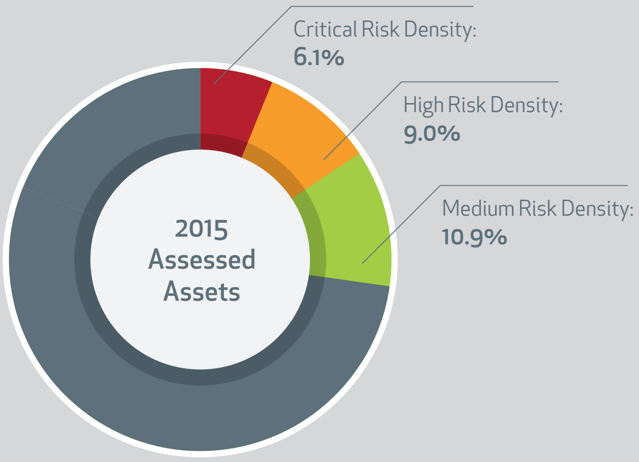


Risk Profile – Hosting/Server Layer



Total (Full-Stack)

Of all assets assessed in 2015 26% of vulnerabilities discovered had a Medium → Critical Risk.



Best practices: Success Stories

In terms of vulnerability mitigation the turnaround time varies depending on where in the stack the discovered vulnerability resides.

It appears patching of systems for known vulnerabilities (CVE's) can be achieved in a relatively short amount of time.

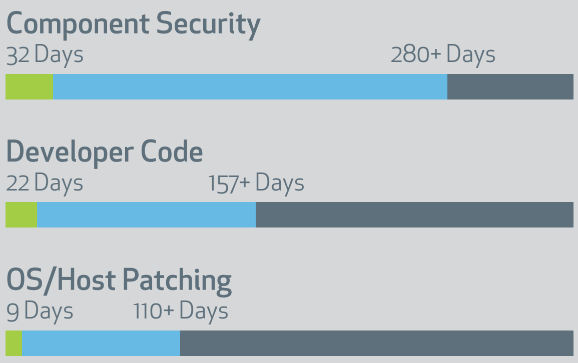
Time-To-Remediation has security significance when looking at the size of the **Window of Exposure** for a given system.

Component Security: Time-To-Remediation appears to take the longest amount of time. This is based on the complexities of retro-fitting new versions of the vulnerable components. It is also understood that many organisations lack a component patching policy and implementing such processes in a live environment is a daunting task.

Developer Code: Time-To-Remediation for code level (developer bugs) vulnerabilities can be fast particularly in the case of new deployments. Older web deployments appear to take more time to remediate mainly due to lack of knowledge of the code-base or the web application not being on the current critical path for the business in terms of assignment of resources to address the issue.

OS/Host Patching : Time-To-Remediation for patching appears to have the fastest turnaround time. This is due apparent and relative ease of applying patches to operating systems and services.

Time-To-Remediation (TTR) for Critical/High Risk issues discovered



Patching & Component Security

Time-To-Remediation for host/OS patching appears to have the fastest turnaround time. This is due to the apparent and relative ease of applying patches to operating systems and services when a critical or important patch is required. Interestingly, patching is never straight forward and needs to be tested in a pre-production environment prior to deploying to live.

- The most common root cause of a vulnerability – poor patching / maintenance
- 63% of vulnerabilities discovered in 2015 could have been avoided if a robust patching, component security policy and/or procedure was implemented
- Over 7.1% of patch related vulnerabilities were Critical or High
- The Patching weaknesses discovered were in relation to operating system and software components, frameworks such as OpenSSL, PHP, Spring, Struts, Apache Server, MySQL, Linux, Windows etc

Recommendation:

- Using "trusted" and commonly used frameworks and components still introduces vulnerabilities into web applications and servers throughno fault of the developers
- Component & Framework security should be a consideration for critical applications at a minimum

SSL/TLS Cryptography

The most common weakness on hosting servers was in relation to SSL (Secure Sockets Layer) or TLS (Transport Layer Security) cryptography and protection of data in transit.

- For every three servers assessed, there was at least two high/medium risk SSL/TLS cryptography issues discovered

In other words, 61.4% of servers were potentially vulnerable to attackers' attempts to attack private communications between web servers and end-user browsers.

For example, in 2015 **edgescan™** reported that 25% of the servers under management assessed were vulnerable to the Poodle (CVE-2014-3566) vulnerability.

SSL is now deprecated and TLS should be used for protecting data in transit.

https://tools.ietf.org/html/rfc7568

2 of every 3 servers contained high-medium risk SSL/TLS cryptography weakness

Client Security - Cross-Site-Scripting (XSS)

Client-side vulnerabilities such as Cross-Site-Scripting (XSS), are a type of attack in which malicious code is injected into otherwise benign and trusted websites. XSS can be used to steal a user's credentials, install malware and redirect end users to questionable websites, etc.

- For every application assessed, **edgescan™** verified an average XSS density of 4.87 per web application
- XSS vulnerabilities were discovered on both web applications and hosting server environments

Remediation: Consider contextual output encoding when rendering or using non trusted data in the client's browser. XSS issues can also occur on the component layer such as framework or service used by the application, patching & maintenance is required to address such issues.

For more see: https://edgescan.com/secure_application_dev_training_material.html

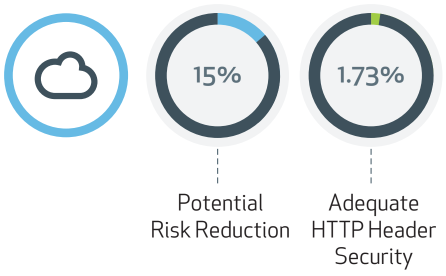
HTTP Security Headers

The lack of Security headers is interesting given how easy they are to implement.

Approximately 15% of application layer vulnerabilities discovered (including some SSL issues) could have been mitigated or risk reduced by using HTTP Security headers. HTTP headers don't affect system performance and simply instruct the user's browser to respect certain conditions of interaction.

Only 1.73% of all Web applications assessed had adequate HTTP Security headers.

For more about security headers see: https://edgescan.com/secure_application_dev_training_material.html



What is edgescan™?

edgescan™ is a managed security service which identifies and provides vulnerability intelligence on an on-going basis. It detects technical vulnerabilities in both internal and Internet facing systems and provides you with the power to understand, prioritise and fix.

It provides you the ability to manage both network and web application security issues for tens, hundreds or even thousands of your systems.

edgescan™ conducts Application & Server vulnerability management with manual validation to help ensure your application & server security.

edgescan™ reports are virtually False Positive free due to our hybrid approach of combining automated testing with manual validation.

edgescan™ provides continuous asset profiling letting you see what systems and services are live and available at any point in time and provides alerting to let you detect rogue, APT or delinquent systems within your asset estate.

edgescan™ gives you:

- Unbeatable price-performance ratio
- Continuous Asset profiling and Alerting
- Continuous vulnerability assessment across both web and hosting layers
- Manual threat verification and accuracy of all issues reported - false positive free
- Prioritisation of security risks and remediation advise from our experts
- 24/7 dashboard access and customisable reporting
- Integration via API/JIRA to plug into your management systems

edgescan™
DIGITAL SECURITY RADAR

False Positve Free,
Full-Stack,
Continuous
Penetration Testing.

"edgescan... identified a large number of application security issues that previously were only identified by our SAST tool..."

edgescan client, March 2015

www.edgescan.com

Gartner

edgescan™

www.bccriskadvisory.com

edgescan™

CONTINUOUS VULNERABILITY MANAGEMENT

Email: info@edgescan.com Telephone: +353 (1) 681 5330
www.edgescan.com