2023 Annual Review

ProCheckUp Ltd

Malaysian Success Team

29th January 2024

Agenda

01. Introduction

An overview of key findings and trends in UK cybersecurity

02. Results from 2023

Detailed findings from the 2023 ProCheckUp clients reports ,including recommendations

03. Client Testimonials

Testimonials from customers of ProCheckUp.

04. Our Team

Team members of ProCheckUp responsible for this annual review.

05. Thank You

Thank you for reading

Introduction

- Welcome to the PCU Annual Trends Review 2023. Today, we delve into the evolving landscape of UK cybersecurity, highlighting key findings and emerging trends.
- Discover insights from our comprehensive analysis of 2023 data, revealing the complexities of today's cyber environments and our innovative approaches to tackling them.

2023 Review Results

Methodology

- **Client Reports Collation**

  We started with a comprehensive collection of data

- **AI Analysis of information garnered**

Leveraging the latest in AI, we performed an in-depth analysis of the collected data.

- **Expert Review and Validation**

Each finding and pattern identified by our AI was meticulously reviewed by cybersecurity experts

- **Reporting**

The final stage involved crafting these insights into this comprehensive report

OWASP Top 10 Summary 2023

- **Security Misconfiguration (33.33%)**

  Most prevalent, with configuration errors potentially leading to data breaches.
- **Software and Data Integrity Failures (14.44%)**

  Concerns about the integrity of software updates and critical data.
- **Identification and Authentication Failures (14.44%)**

  Significant challenges in accurately managing user identities and authentications.
- **Injection (10.37%)**

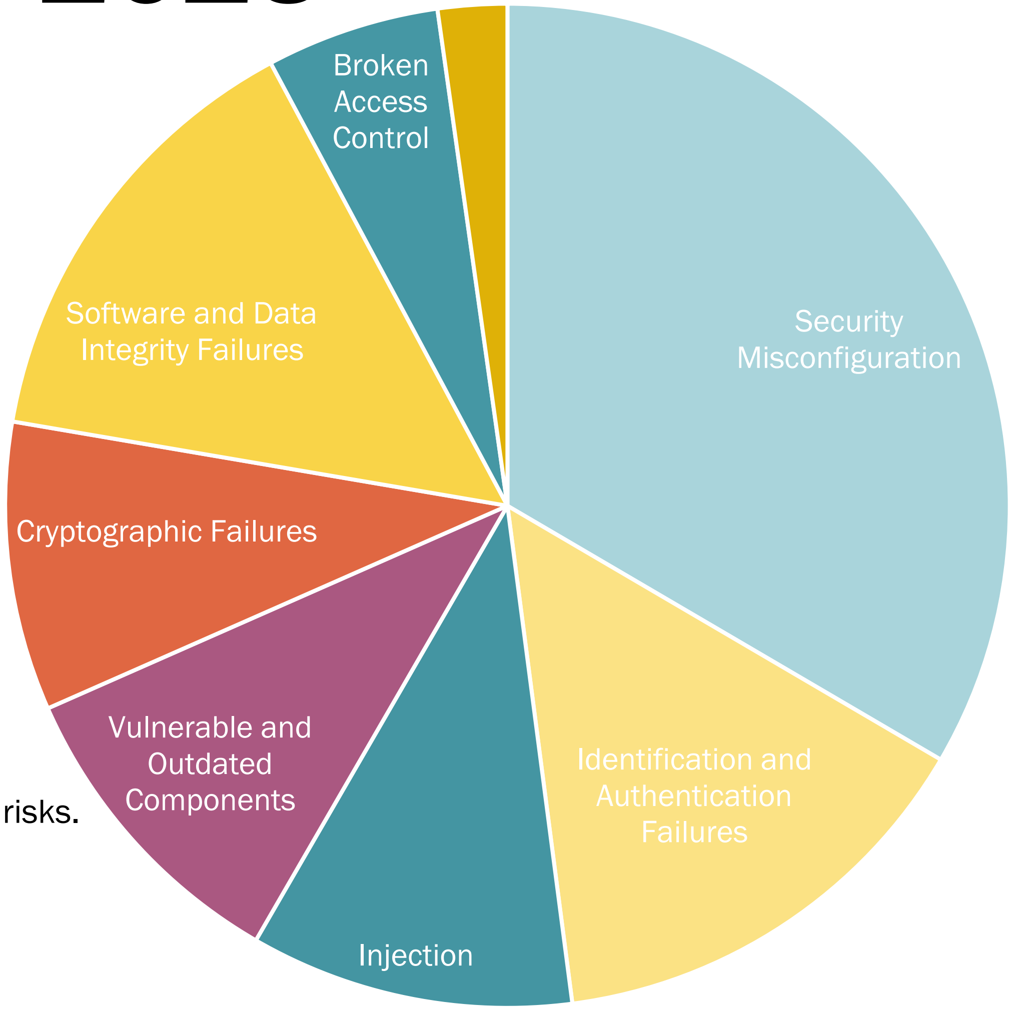
  High-risk injection flaws that can manipulate backend systems.
- **Vulnerable and Outdated Components (10.00%)**

  Risks associated with using components that have known security vulnerabilities.
- **Cryptographic Failures (9.26%)**

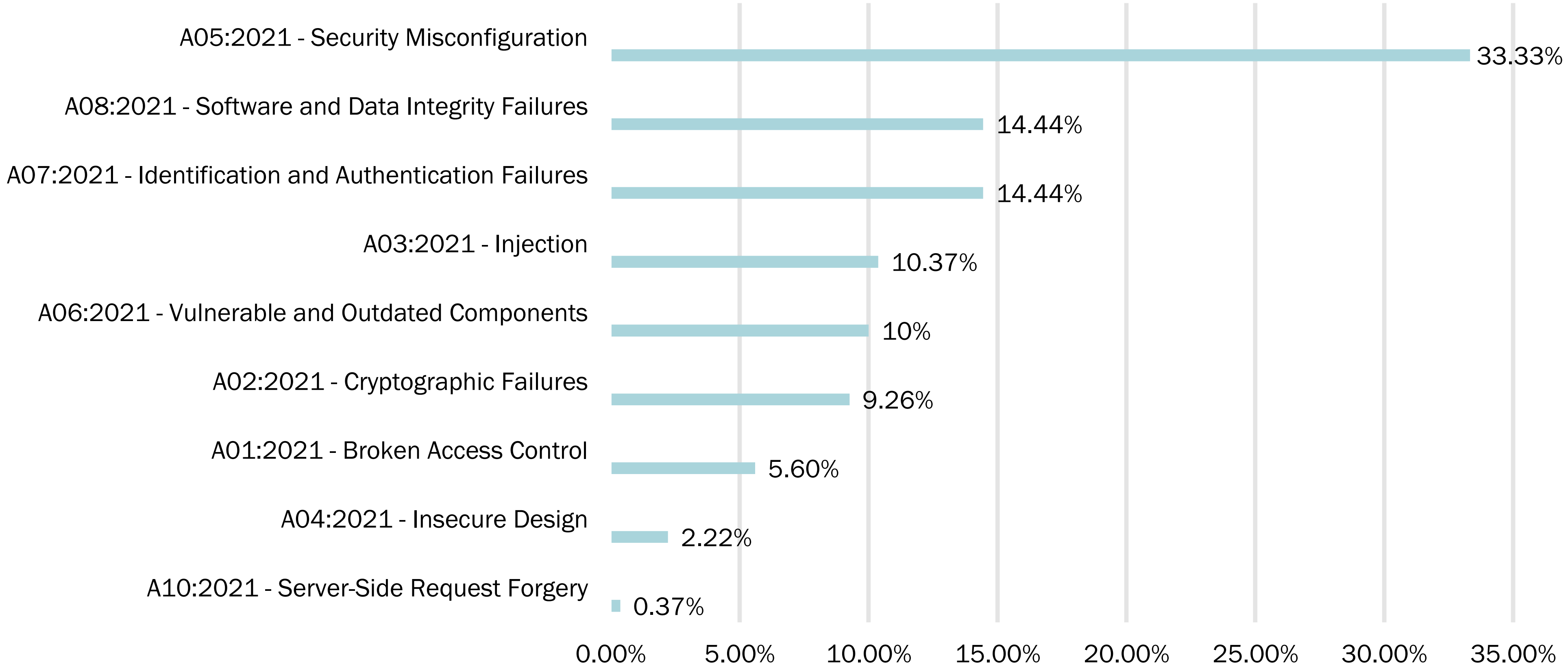
  Weak or improper cryptographic practices compromising data protection.
- **Broken Access Control (5.56%)**

  Challenges in enforcing user access restrictions, leading to unauthorized data access risks.
- **Insecure Design (2.22%)**

  Vulnerabilities due to flawed or inadequate security design.



OWASP Top Ten 2023 Findings (Percentage)



A05:2021 - Security Misconfig (33.3%)

- **Definition:** Security Misconfiguration happens when security settings are defined, implemented, and maintained inadequately. It can occur at any level of an application stack, including network services, platforms, web servers, databases, applications, etc.
- **Impact:** With a substantial percentage of 33.3%, this is indicative of a widespread problem. Misconfigurations can lead to unauthorised access and data breaches.
- **Mitigation Strategies:**

  Regular, automated scanning for misconfigurations across all parts of the application stack.

  Implementation of a secure installation process including minimal platforms without unnecessary features, components, documentation, and samples.

  Continuous review and hardening of system configurations.

A08:2021 - Software and Data Integrity Failures (14.4%)

- **Definition:** This category refers to making assumptions about software updates, critical data, and CI/CD pipelines without verifying integrity. Attackers can manipulate insecure software updates or data to distribute malicious components or manipulate systems.
- **Impact:** With 14.4% of total issues found, this indicates a substantial risk associated with unverified software or corrupted data.
- **Mitigation Strategies:**

  Use digital signatures or similar mechanisms to verify the integrity of software and data.

  Implement a secure CI/CD pipeline.

  Regularly review and test the integrity of data and software updates.

A07:2021 - Identification and Authentication Failures (14.4%)

- **Definition:** These failures occur when functionalities related to identity management and authentication are implemented incorrectly, allowing attackers to compromise passwords, keys, session tokens, or exploit other implementation flaws to assume other users' identities.
- **Impact:** With 14.4% of total issues found, this area is particularly vulnerable, potentially leading to unauthorised access and breaches.
- **Mitigation Strategies:**

  Implement multi-factor authentication.

  Ensure secure password management practices.

  Regularly audit and update authentication mechanisms.

A03:2021 - Injection (10.4%)

- **Definition:** Injection flaws, such as SQL, NoSQL, Command Injection, etc., occur when untrusted data is sent to an interpreter as part of a command or query. Attackers can use these flaws to access unauthorized data or execute malicious commands.
- **Impact:** The high percentage of issues found 10.4% indicates a critical vulnerability, potentially allowing attackers to gain control over backend systems.
- **Mitigation Strategies:**

  Use of prepared statements (with parameterised queries) in SQL code.

  Employing ORM (Object Relational Mapping) frameworks which are less prone to injection.

  Regularly testing code for injection vulnerabilities using automated tools.

A06:2021 - Vulnerable and Outdated Components (10%)

- **Definition:** This category involves using components with known vulnerabilities, such as libraries, frameworks, and other software modules. When unpatched, these components can compromise the entire application.
- **Impact:** The identification of 10% of issues found in this category signifies a significant risk due to outdated or vulnerable components that could be exploited by attackers.
- **Mitigation Strategies:**

  Regularly update and patch all components.

  Remove unused dependencies and unnecessary features.

  Conduct automated scanning to identify and address vulnerabilities in components.

A02:2021 - Cryptographic Failures (9.26%)

- **Definition:** Previously known as "Sensitive Data Exposure," Cryptographic Failures focus on the protection of data in transit and at rest. Issues arise when sensitive data is not adequately encrypted or when outdated or weak cryptographic algorithms are used.
- **Impact:** The presence of 9.26% issues found indicates a substantial risk of sensitive data, such as personal information, credentials, or credit card details, being exposed and potentially exploited.
- **Mitigation Strategies:**

Ensure the use of strong, up-to-date cryptographic algorithms.

Encrypt all sensitive data at rest and in transit.

Regularly update and patch systems to avoid known vulnerabilities in cryptographic libraries.

A01:2021 - Broken Access Control (5.56%)

Definition: Broken Access Control occurs when restrictions on what authenticated users are allowed to do are not properly enforced. It allows attackers to exploit these flaws to access unauthorised functionality and data, such as accessing other users' accounts, viewing sensitive files, modifying other users' data, and changing access rights.

Impact: With 5.56% of issues identified, this suggests a significant risk in ensuring only authorised users can access certain data or functionalities. This can lead to data breaches, unauthorized data manipulation, and compromise of the entire system.

Mitigation Strategies:

Implement access control mechanisms that are enforced in server-side code.

Use a minimal privilege approach, ensuring users have the least access necessary.

Continuously review and update access control rules in light of new functionalities or changes in business requirements.

A04:2021 - Insecure Design (2.22%)

- **Definition:** Insecure Design refers to risks associated with missing or ineffective control design, leading to a wide range of security issues.
- **Impact:** Although only comprising 2.22% of the issues found, these can have widespread effects, leading to systemic security flaws.
- **Mitigation Strategies:**

  Adopt a 'security by design' philosophy.

  Conduct threat modelling for critical applications and functionalities.

  Regularly review and update the design based on evolving security threats.

2023 Management Vulnerability Summary

Server and System Maintenance (36.9%): Predominant issues in server setup and maintenance, signalling the need for enhanced patch management and system updates.

Application and Development Security (28.5%): Significant vulnerabilities in coding, deployment, and maintenance of applications, emphasizing the need for secure development practices.

Network and Infrastructure Security (18.5%): Concerns in network configuration and perimeter defences, highlighting risks in infrastructure security.

Access Control and Data Protection (13.1%): Challenges in managing user access and protecting sensitive data, underscoring the importance of robust access control mechanisms.

Security Policy and Third-party Risks (3%): Fewer but impactful issues related to adherence to security policies and the management of third-party risks, stressing the need for vigilant policy enforcement and vendor assessments.

Management Categories Used

- **Network and Infrastructure Security**

Combines infrastructure management issues and firewall management, focusing on vulnerabilities related to network configurations, perimeter defences, and overall infrastructure security.

- **Server and System Maintenance**

Merges server configuration issues and server management/patching issues. This category addresses vulnerabilities arising from improper server setup, lack of regular maintenance, outdated systems, and failure to apply security patches.

- **Application and Development Security**

Encompasses programming issues, application deployment, and maintenance concerns. This category deals with vulnerabilities stemming from coding flaws, insecure application deployment, and inadequate application maintenance practices.

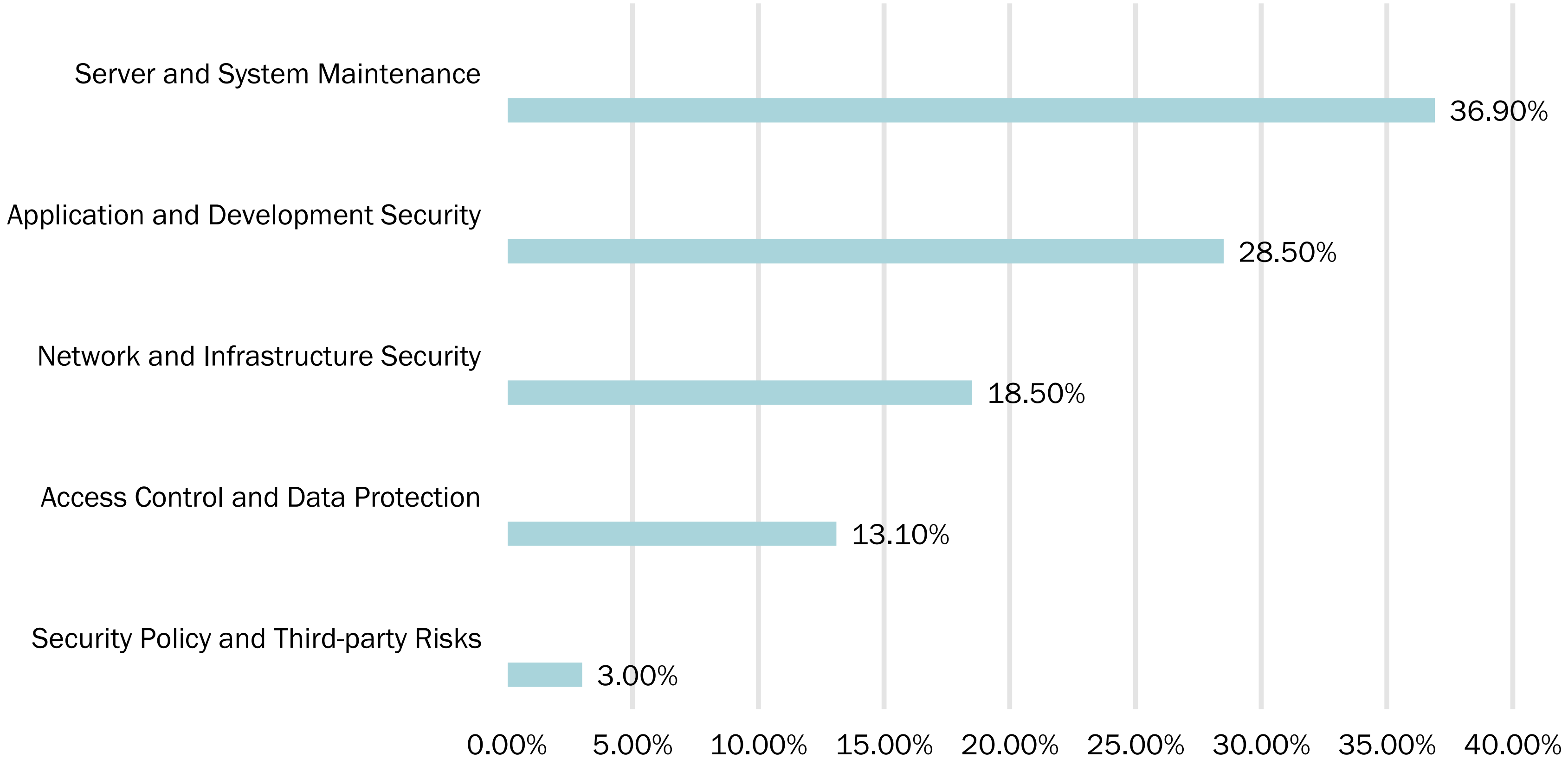
- **Access Control and Data Protection**

Combines access control, authentication management, and data protection/encryption failures. It focuses on vulnerabilities related to user access management, authentication system weaknesses, and failures in protecting sensitive data.

- **Security Policy and Third-party Risks**

Merges security policy/compliance issues and third-party/vendor management issues. This category highlights vulnerabilities associated with non-adherence to security policies, compliance lapses, and risks introduced by third-party services and external dependencies.

Management Vulnerabilities Categories



Server and System Maintenance (36.9%)

- **Description:** Focuses on the predominant issues in server setup and maintenance. This section underscores the necessity of enhanced patch management and system updates.
- **Implications:** With 36.9% of issues found, there is a pressing need for rigorous and proactive server and system maintenance protocols.
- **Actionable Recommendations:**

  Implementation of a systematic server maintenance schedule.

  Regular updates and patching of all server components.

  Continuous monitoring for system health and security updates.

Application and Development Security (28.5%)

- **Description:** This slide focuses on vulnerabilities in coding, deployment, and maintenance of applications. It emphasizes the importance of secure development practices.
- **Implications:** The high percentage of 28.5% of the issues highlights significant risks in application security, particularly in the areas of coding practices and deployment strategies.
- **Actionable Recommendations:**

Adopt secure coding standards and regular code reviews.

Implement security-focused development lifecycle processes.

Conduct regular security assessments and penetration testing on applications.

Network and Infrastructure Security (18.5%)

- **Description:** This section addresses vulnerabilities related to network configurations and perimeter defences. It highlights the risks in infrastructure security that can lead to unauthorized access and potential data breaches.
- **Implications:** The identification of 18.5% of the issues underlines the critical need for robust network security measures.
- **Actionable Recommendations:**

Regular audits and updates of network configurations.

Strengthening perimeter defences with advanced security solutions.

Continuous monitoring for potential vulnerabilities and threats.

Access Control and Data Protection (13.1%)

- **Description:** Addresses challenges in managing user access and protecting sensitive data, emphasizing the need for robust access control and data encryption.
- **Implications: Comprising** 13.1% of the issues, this indicates potential vulnerabilities in access management systems and data protection protocols.
- **Actionable Recommendations:**

  Strengthen user authentication and authorization processes.

  Implement encryption for sensitive data both in transit and at rest.

  Regularly review and update access control policies and procedures.

Security Policy and Third-party Risks (3%)

- **Description:** Focuses on vulnerabilities related to adherence to security policies and the management of third-party risks. Though fewer in number, these issues can have a significant impact.
- **Implications:** Comprising 3% of the issues found, these stress the importance of maintaining strict compliance with security policies and managing third-party vendor risks effectively.
- **Actionable Recommendations:**

  Regular audits for policy compliance and third-party risk assessments.

  Develop and enforce strict security protocols for vendor management.

  Provide ongoing training and awareness programs on security policy adherence.

Client Testimonials

Client Successes –

“

Cyber Essential Plus

Efficient, engaging, helpful, no suggestions for improvement, I was very happy with this work and look forward to our next assessment with ProCheckUp

Pharmaceuticals Research Organisation

Client Successes –

“

Firewall Review

Excellent with all aspects of the engagement, Sales team always goes the extra mile to help with all engagements, all consultants are professional.

Global Food Delivery Leader

Client Successes –

“

Web Application

Exceptional customer service provided. Thank you ProCheckUp.

Innovative Tech Solutions Provider

Our Team

Four out of thirty: Malaysian Team members who compiled the report

Gurichha

Security Consultant: Pioneering innovative security solutions.

Arassh

Marketing & Operations

Mohin

Security Consultant: Expert in vulnerability assessment and risk management.

Loh Shyan

Security Consultant: Expert in vulnerability assessment and risk management.

Thank you

Your commitment fuels our passion for cybersecurity excellence.

Join us on our journey - subscribe to our newsletter for the latest in cyber trends and follow us on

https://www.linkedin.com/company/procheckup-ltd

https://twitter.com/procheckup

ProCheckUp

sales@procheckup.com