FAO Danny Werb

Computing, Digital Forensics and Cybersecurity

BSc (Hons). Computing Forensics and Security

2023-2024

IS 40

Title: Evaluation of penetration testing reporting methods using CVSS4.0

Author: Marco Carrasco Talán

E-mail: [mc1381@canterbury.ac.uk](mailto:mc1381@canterbury.ac.uk)

This report is submitted in partial fulfilment of the requirement for  
the BSc in Computing Forensics and Security at Canterbury Christ Church University

I declare that this report is my own original work containing no personal data as defined in the Data Protection Act (1998) and that I have read, understood and accept the University's regulations on plagiarism/intellectual property rights/research ethics (in particular the Research Governance Handbook) and the IS 40 Module Handbook

Further, I accept that digital and/or hard copies of my Individual Study 40, or parts thereof,  
may be made available to other students, individuals and organisations after it has been  
marked.  
Finally, I accept that no copy of my Individual Study 40 will ever be returned regardless of  
the circumstances

Signed: Un dibujo de una persona

Descripción generada automáticamente con confianza media

Date of Submission: 12/04/2024

Acknowledgment

I would like to thank my supervisor Danny Werb for being patient with me, helping me through the whole process and making this research academic quality. And for all his positive contributions to improve the research.

I would also like to thank Katherine Duque for her daily support and help with the research, your support has been necessary for the success of this research.

Finally, I would like to thank my parents for giving me the opportunity to study at CCCU and for putting their trust in me.

This study addressed the standardisation of penetration testing reports using the CVSS 4.0 scoring system, using a quantitative methodology. To this end, a survey was designed for five cybersecurity professionals to assess the effectiveness and acceptability of a standardised report. The results obtained indicated that the use of templates hosted on platforms such as Google Docs and OneDrive significantly facilitated the preparation and access to the reports. In addition, it was determined that reports should not be excessively long, as brevity and clarity were essential for effective communication of penetration testing results.

The proposed standardised report developed in this study was positively evaluated by the practitioners surveyed, who highlighted that it met most of the organisational requirements. These requirements included clarity, accessibility and the ability to provide accurate and relevant information on the vulnerabilities assessed.

Content

[Appendix A: Glossary 7](#_Toc166447129)

[List of Figures 8](#_Toc166447130)

[List of tables 10](#_Toc166447131)

[1 Introduction 11](#_Toc166447132)

[Objective and potential improvements 11](#_Toc166447133)

[Hypothesis: 12](#_Toc166447134)

[2 Literature review 13](#_Toc166447135)

[2.1 What is OWASP top 10 13](#_Toc166447136)

[2.2 Importance of OWASP top 10 in web applications 13](#_Toc166447137)

[2.3.1 A1 Broken Access control: 14](#_Toc166447138)

[2.3.2 A2 Cryptographic failures 14](#_Toc166447139)

[2.3.3 A3 Injection 14](#_Toc166447140)

[2.3.4 A4 Insecure design 14](#_Toc166447141)

[2.3.5 A5 Security misconfiguration 14](#_Toc166447142)

[2.3.6 A6 Vulnerable and outdated components 15](#_Toc166447143)

[2.3.7 A7 Identification and Authentication Failures 15](#_Toc166447144)

[2.3.8 A8 Software and Data Integrity Failures 15](#_Toc166447145)

[2.3.9 A9 Security Logging 15](#_Toc166447146)

[2.3.10 A10 SSRF 15](#_Toc166447147)

[2.3 CVSS4.0 16](#_Toc166447148)

[2.3.1 What is CVSS 16](#_Toc166447149)

[2.4 Upgrades of CVSS4.0 16](#_Toc166447150)

[2.5 Comparison between CVSS4.0 and CVSS3.1 16](#_Toc166447151)

[2.6 Example of vulnerability measured using CVSS4.0 17](#_Toc166447152)

[3 Main Chapter 21](#_Toc166447153)

[3.1 Analysis of PwnDoc 21](#_Toc166447154)

[3.2 What is PwnDoc: 21](#_Toc166447155)

[3.2.1 Features of PwnDoc: 21](#_Toc166447156)

[3.3 How to configure PwnDoc: 22](#_Toc166447157)

[3.4 Setting of languages and types of audits 23](#_Toc166447158)

[3.5 Limitations of PwnDoc: 31](#_Toc166447159)

[3.6 Introduction of reporting methodologies: 32](#_Toc166447160)

[3.7 Phases of a report: 32](#_Toc166447161)

[3.8 Contents of a standard report 33](#_Toc166447162)

[3.8.1 1º Executive Summary 33](#_Toc166447163)

[3.8.2 2º Project Objective 35](#_Toc166447164)

[3.8.3 3º Timeline 37](#_Toc166447165)

[3.8.4 4º Summary of findings 39](#_Toc166447166)

[3.8.5 5º Summary of recommendations 42](#_Toc166447167)

[3.8.6 6º Example of a description of findings: 44](#_Toc166447168)

[3.9 Proposal of the standard with improvements 49](#_Toc166447169)

[3.10 Example of a report with proposed improvements 50](#_Toc166447170)

[3.11 Professional Survey 51](#_Toc166447171)

[3.11.1 Survey objective and questions 51](#_Toc166447172)

[4 Legal Considerations 52](#_Toc166447173)

[5 Ethical Considerations 53](#_Toc166447174)

[6 Methodology /Methods 54](#_Toc166447175)

[7 Findings 55](#_Toc166447176)

[7.1Automatic Vs Manual reporting 55](#_Toc166447177)

[7.2 Report Writing 56](#_Toc166447178)

[8 Evaluation 63](#_Toc166447179)

[9 Discussion 64](#_Toc166447180)

[9.1 Evaluation of the literature 64](#_Toc166447181)

[9.2Assessment of the methodology 64](#_Toc166447182)

[9.3Evaluation of the main key findings 64](#_Toc166447183)

[9.3.1Manual vs. automated reporting 64](#_Toc166447184)

[9.3.2Reporting methods 64](#_Toc166447185)

[9.3.4 Survey 65](#_Toc166447186)

[9.4 Results 65](#_Toc166447187)

[10 Conclusion 66](#_Toc166447188)

[References 67](#_Toc166447189)

[Appendices 70](#_Toc166447190)

[Appendix B: Marking Scheme 70](#_Toc166447191)

[Appendix C: Changes to research proposal 71](#_Toc166447192)

[The focus of the research was changed, originally it was going to investigate the implementation of AI Prompts, in the research this part of the research has been eliminated.  71](#_Toc166447193)

[Appendix D: Project Management 72](#_Toc166447194)

[Appendix E: Meetings With supervisor 73](#_Toc166447195)

[Appendix F: Survey Questionnaire 74](#_Toc166447196)

[Appendix G: Participant Information Sheet: 75](#_Toc166447197)

[**Background** 75](#_Toc166447198)

[*Be a cybersecurity professional, with at least 1 year working / bug bounty experience, or in a similar management position, with certifications, or active in ethical hacking communities.* 75](#_Toc166447199)

[**Procedures** 75](#_Toc166447200)

[Appendix H: Survey answers 77](#_Toc166447201)

[Appendix H1: Professional1: 77](#_Toc166447202)

[Appendix H2: Professional 2 79](#_Toc166447203)

[Appendix H3: Professional 3 80](#_Toc166447204)

[Appendix H4: Professional 4 81](#_Toc166447205)

[Appendix H5: Professional 5 82](#_Toc166447206)

[Appendix I: Consent Form 83](#_Toc166447207)

[Appendix I1: Consent form 1: 83](#_Toc166447208)

[Appendix I2: Consent form 2 85](#_Toc166447209)

[Appendix I3: Consent form 3 87](#_Toc166447210)

[Appendix I4: Consent form 4 89](#_Toc166447211)

[Appendix I5: Consent Form 5 91](#_Toc166447212)

[Appendix J: Research Questions 93](#_Toc166447213)

[Appendix K: Evaluation 95](#_Toc166447214)

# Appendix A: Glossary

OWASP: Open Web Application Security Project

CVSS: Common Vulnerability Scoring System

CVE: Common Vulnerability Exposure

IDOR: Insecure Direct

SQL: Structured Query Language

SSRF: Server Side Request Forgery

ACL: Access control list

PoC: Proof of Concept

IEEE: Institute of Electrical and Electronics Engineers

NIST: National Institute of Standards and Technology

GDPR: general data protection regulation

ICS System: type of control system used for industrial processes, including systems like supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other smaller control system configurations. These systems are used to control and monitor industrial processes, such as manufacturing, production, and utility operations.

OT System: Operational Technology (OT) systems refer to hardware and software that detect or cause changes through direct monitoring and control of physical devices, processes, and events in industrial environments. Unlike Information Technology (IT) systems, which manage data and information processing, OT systems are focused on the operation of machinery and physical processes.

SSRF: Server Side Request Forgery.

# List of Figures

[Figure 1 OWASP top 10 (OWASP, no-date) 13](#_Toc166447215)

[Figure 2 Base metrics (Common Vulnerability Scoring System Version 4.0 Calculator, no date) 17](#_Toc166447216)

[Figure 3 Supplemental Metrics (Common Vulnerability Scoring System Version 4.0 Calculator, no date) 18](#_Toc166447217)

[Figure 4 Environmental (Modified Base Metrics) (Common Vulnerability Scoring System Version 4.0 Calculator, no date) 19](#_Toc166447218)

[Figure 5 Environmental (Security Metrics) (Common Vulnerability Scoring System Version 4.0 Calculator, no date) 19](#_Toc166447219)

[Figure 6 Threat Metrics (Common Vulnerability Scoring System Version 4.0 Calculator, no date) 19](#_Toc166447220)

[Figure 7 Configuration of languages and audit types (yeln4ts, no-date). 22](#_Toc166447221)

[Figure 8 List of languages(yeln4ts, no-date). 23](#_Toc166447222)

[Figure 9 Template Uploading (yeln4ts, no-date). 23](#_Toc166447223)

[Figure 10 Clients database(yeln4ts, no-date). 23](#_Toc166447224)

[Figure 11 Companies Database(yeln4ts, no-date). 23](#_Toc166447225)

[Figure 12 Add collaborators(yeln4ts, no-date). 24](#_Toc166447226)

[Figure 13 Creating Vulnerability types(yeln4ts, no-date). 24](#_Toc166447227)

[Figure 14 Creating Vulnerability Category(yeln4ts, no-date). 25](#_Toc166447228)

[Figure 15 Creating Audit type (yeln4ts, no-date). 25](#_Toc166447229)

[Figure 16 Creating audit (yeln4ts, no-date). 26](#_Toc166447230)

[Figure 17 Configuring the new Audit(yeln4ts, no-date). 26](#_Toc166447231)

[Figure 18 Vulnerability selection(yeln4ts, no-date). 27](#_Toc166447232)

[Figure 19 Proofs Section (yeln4ts, no-date). 27](#_Toc166447233)

[Figure 20 Details Section (yeln4ts, no-date). 28](#_Toc166447234)

[Figure 21 XSS vulnerability of the report (yeln4ts, no-date). 28](#_Toc166447235)

[Figure 22 XSS part 2 (yeln4ts, no-date). 29](#_Toc166447236)

[Figure 23 Vulnerabilities Summary (yeln4ts, no-date). 29](#_Toc166447237)

[Figure 24 General information (yeln4ts, no-date). 30](#_Toc166447238)

[Figure 25 Modifications history (yeln4ts, no-date). 30](#_Toc166447239)

[Figure 26 Example of table formatting in report template (yeln4ts, no-date). 31](#_Toc166447240)

[Figure 27 Offensive Security Executive Summary (Offensive Security Services, LLC, 2013). 33](#_Toc166447241)

[Figure 28 Disclosed Report Executive Summary (ACK-J, 2023). 34](#_Toc166447242)

[Figure 29 Project Objective of Disclosed report(ACK-J, 2023). 35](#_Toc166447243)

[Figure 30 Scope of GitHub disclosed report (ACK-J, 2023). 35](#_Toc166447244)

[Figure 31 Methodology of GitHub Report (ACK-J, 2023). 36](#_Toc166447245)

[Figure 32 Timeline of disclosed report part 1 (ACK-J, 2023). 37](#_Toc166447246)

[Figure 33 Timeline of disclosed report part 2 (ACK-J, 2023). 38](#_Toc166447247)

[Figure 34 Summary of findings in Offensive Security Report (Offensive Security Services, LLC, 2013). 39](#_Toc166447248)

[Figure 35 Index of the report (ACK-J, 2023) 39](#_Toc166447249)

[Figure 36 Key findings of GitHub disclosed report (ACK-J, 2023) 40](#_Toc166447250)

[Figure 37 Statistics section of GitHub report (ACK-J, 2023) 40](#_Toc166447251)

[Figure 38 Vulnerabilities measured by TTPs (ACK-J, 2023) 41](#_Toc166447252)

[Figure 39 Summary of recommendations in Offensive Security report (Offensive Security Services, LLC, 2013) 42](#_Toc166447253)

[Figure 40 Example of mitigation in GitHub disclosed report (ACK-J, 2023) 43](#_Toc166447254)

[Figure 41 References of GitHub disclosed report (ACK-J, 2023) 43](#_Toc166447255)

[Figure 42 “Attack Narrative” Index in Offensive Security Disclosed report (Offensive Security Services, LLC, 2013) 45](#_Toc166447256)

[Figure 43 Example of narrative reporting in Offensive Security Report (Offensive Security Services, LLC, 2013) 45](#_Toc166447257)

[Figure 44 Organization of findings in GitHub disclosed report (ACK-J, 2023) 46](#_Toc166447258)

[Figure 45 Replication section of GitHub disclosed report (ACK-J, 2023) 47](#_Toc166447259)

[Figure 46 Mitigation and references of GitHub Disclosed report (ACK-J, 2023) 48](#_Toc166447260)

[Figure 47 Question 2 58](#_Toc166447261)

[Figure 48 Question 4 59](#_Toc166447262)

[Figure 49 Question 6 59](#_Toc166447263)

[Figure 50 Question 8 60](#_Toc166447264)

[Figure 51 Question 9 60](#_Toc166447265)

[Figure 52 Question 10 61](#_Toc166447266)

[Figure 53 Gantt Chart 72](#_Toc166447267)

# List of tables

[Table 1 Report Improvements 49](#_Toc166447268)

[Table 2 Example of report 50](#_Toc166447269)

[Table 4 Comparison of reporting methods 57](#_Toc166447270)

[Table 5 Positive and negative aspects of the report 62](#_Toc166447271)

[Table 7 Professional 1 77](#_Toc166447272)

[Table 8 Professional 2 79](#_Toc166447273)

[Table 9 Professional 3 80](#_Toc166447274)

[Table 10 Professional 4 81](#_Toc166447275)

[Table 11 Professional 5 82](#_Toc166447276)

# 1 Introduction

Since cybersecurity is a job, vulnerabilities have been tried to be categorized and measured to perform a triage in order to select which of them need to be fixed as soon as possible, first CVE (Common Vulnerability Exposure) was founded in 1999 to categorize vulnerabilities. After that in 2005 a way to categorize vulnerabilities to be applied to reports was created, this is called CVSS.

Currently in 2023 the documents and the content of the reports are standardized, but it is not given too much depth in what to put nor an example to look at, and with the recent update of CVSS it is positive to try to integrate version 4.0 to the reports. Nowadays there are only 2 major research papers published in IEEE.

IEEE managed not only to standardize the content of the report but also the process of a penetration testing, but only the phases are specified, it does not standardize the tools that can be used at each and also does not focus on web applications, only on generic penetration testing(Alghamdi, 2021).

## Objective and potential improvements

A report should not only detail which vulnerabilities have been found in which sites, and a short executive summary where it briefly explains what happened, the report should also be cross-cutting.

This means that it can be useful both for the programmer who fixes the site and for the CISO who is reading the report, with this what is proposed is that with a series of measures for writing reports and guidelines to follow, a centralized resource is created and additional resources so that each role has what it needs to make its job easier.

Another reason for doing this research is to learn about CVSS 4.0 and how no could be implemented in reporting.

The purpose of this study is to investigate how to standardize the way vulnerability reporting is done in web applications, the study plans to answer the following questions.

* What would a report using the new CVSS4.0 (instead of the classic CVSS 3.1) look like?
* How could the process of reporting be standardized?
* Is it effective to create a framework for reporting?
* Are the automatic reporting tools easy to understand?

The objective to answer these questions is to analyse the new CVSS4.0 vulnerability metrics system, use and critically analyse an open-source automatic reporting tool and create a series of steps and objectives to deliver reports and then based on all of that give it to 10 penetration testers to give their opinion on the feasibility.

Other purposes to do the research and propose a solution:

1º Personal experience: Having worked for a while in a major telecommunications and cybersecurity company in Spain I have seen the lack of communication, coordination when performing audits and also when presenting the report to the client, customers sometimes complained because it was not very clear that the vulnerability existed, besides that in very few cases there were false positives and that was not checked.

2º Problem of communication in Spanish IT companies: Poor communication between managers who do not have technical knowledge and IT and security teams can affect the decisions and cyberattacks they receive, therefore a good response from the penetration testing team, so a good report can help senior management understand what happens and technical teams can patch vulnerable assets (Redaccion, 2023).

## Hypothesis:

The creation of an effective and efficient reporting method may enhance cyber decision-making in companies. This improvement could lead to better prevention of cyber-attacks and cost savings through securing infrastructure. The aim is to create an effective reporting method to improve decision-making, enhance cybersecurity, and reduce infrastructure security costs.

# 2 Literature review

## 2.1 What is OWASP top 10

The OWASP Top 10 is a project that identifies and ranks the top ten web application security vulnerabilities. This list is updated regularly and is recognized worldwide by developers as the first step towards more secure web coding.

The OWASP Top 10 focuses on identifying the most critical and common security issues that can affect web applications. Each security issue included in the list represents a broad consensus on the most critical security risks to web applications.

## 2.2 Importance of OWASP top 10 in web applications

The OWASP top 10 is very important when it comes to code development and auditing.

When developing code, it always has to pass a security check before it can be released. OWASP top 10 is the reference framework used by programmers in development cycles.

When performing bug bounty or penetration testing exercises, the OWASP top 10 helps companies to categorize the criticality of the vulnerabilities found, since a code injection is different from an information leak.

Other reasons why the OWASP is necessary in cybersecurity

* 1. Awareness: The OWASP Top 10 helps raise awareness of the most critical threats and vulnerabilities
* 2. Security prioritization: By providing a list of the top ten vulnerabilities, the OWASP Top 10 allows organizations to prioritize their security efforts. This can be especially useful for organizations with limited resources.
* 3. Improved coding practices: By understanding the most common vulnerabilities, developers can improve their coding practices to avoid these problems.
* 4. Compliance with regulations: Many security regulations and standards, such as the Payment Card Industry Data Security Standard (PCI DSS), require organizations to adhere to the OWASP Top 10
* 5. Risk reduction: By addressing OWASP Top 10 vulnerabilities, organizations can significantly reduce their risk profile. This can result in a reduced likelihood of suffering a security breach (OWASP, no-date).

Diagrama

Descripción generada automáticamente

Figure 1 OWASP top 10 (OWASP, no-date)

### 2.3.1 A1 Broken Access control:

In first position we have vulnerabilities related to failures in access and validation controls in applications.

This failure can cause unauthorized access, information leaks, modification of sensitive data or gaining privileges in the system illicitly (OWASP, no-date).

A very common and simple attack is the IDOR attack.

Suppose you have an e-commerce web application. Users can view their own orders and order details by accessing a specific URL, such as https://[www.shop.com/my\_orders/<ORDER\_ID](http://www.shop.com/my_orders/%3cORDER_ID)>.

A user can normally only view their own orders since the application verifies their identity before displaying the order information. However, if the application has broken access control, a user might be able to view other users’ orders simply by changing the <ORDER\_ID> in the URL (PortSwigger, no date).

This vulnerability is very simple to understand and requires no technical knowledge.

### 2.3.2 A2 Cryptographic failures

This section are vulnerabilities related to the lack of privacy or security in the transmissions in the application, it is related to failures in the cryptographic algorithms used by the applications to transmit information, or critical information that is not completely secure.

A possible scenario would be a database that does not have hashed passwords, or that the cryptographic protocols used by the web application are outdated (OWASP, no-date).

### 2.3.3 A3 Injection

These vulnerabilities are very common, as they involve the application being able to inject code, or the application interpreting the executed code to perform malicious actions on the application.

One of the most famous attacks in this section is SQL injection.

An example of a possible scenario:

A user registration application does not control the inputs it receives, and the user can manipulate the database and alter it, since not only does it not control the input it receives, but the account that controls the database has sufficient privileges to manipulate the database (OWASP, no-date).

### 2.3.4 A4 Insecure design

This section discusses the concept of unsafe design in application development, distinguishing it from unsafe implementation. Unsafe design refers to inherent weaknesses due to missing or ineffective security controls that cannot be remedied by flawless implementation. For example, a web application for an online store might have a search function designed without considering potential exploitation by attackers, such as using the search to access sensitive user information. (OWASP, no-date).

### 2.3.5 A5 Security misconfiguration

Incorrect security settings can include a variety of problems, such as unnecessary features enabled or installed, default accounts and their passwords still enabled and unchanged, error handling that reveals stack traces or other overly informative error messages to users, updated systems whose latest security features are disabled or not securely configured, among others.

One scenario would be an application that has directory listing enabled, allowing attackers to exfiltrate information and get server configuration files (OWASP, no-date).

### 2.3.6 A6 Vulnerable and outdated components

This section refers to whether the components used by an application are outdated, deprecated or obsolete.

An example scenario would be an application that has an outdated library, making it vulnerable and making possible attacks (OWASP, no-date).

### 2.3.7 A7 Identification and Authentication Failures

This section focuses on attacks that can result in the loss of identification of the victim user.

An example scenario would be the use of passwords as the only authentication method, or the credential stuffing attack, an attack in which a list of users and passwords is used in the login to validate whether they exist or not (OWASP, no-date).

### 2.3.8 A8 Software and Data Integrity Failures

This section focuses on the use of vulnerable components or technologies, it is different from A6 since A6 focuses on bugs due to outdated software.

A possible scenario would be that when building an application a library is used that is vulnerable (OWASP, no-date).

### 2.3.9 A9 Security Logging

This section focuses on failures in the logging and monitoring of application activities.

An example of this would be that the event monitor of an application fails to detect that a brute force attack is being made (OWASP, no-date).

### 2.3.10 A10 SSRF

This category itself is an attack.

In a few words the failures produced by SSFR occur when a user, abusing the trust of the application, manages to obtain internal resources of the server, falsifying the legitimacy of the request and overcoming defensive barriers such as ACLs or firewalls.

An example of this would be a user in an online file management system, in the search URL searching the URL <http://localhost/admin> can manage to obtain content from that URL (OWASP, no-date).

## 2.3 CVSS4.0

### 2.3.1 What is CVSS

CVSS (Common Vulnerability Scoring System) is a scoring system that classifies the criticality of vulnerabilities, allowing to generate a score based on their main characteristics. This scoring system is designed to provide an open and standard method for estimating the impact of identified IT vulnerabilities. In other words, it helps to quantify the severity that such vulnerabilities may represent.

CVSS uses three groups of metrics to calculate a score associated with a vulnerability: base, temporal and environment. Base metrics represent the characteristics intrinsic to the vulnerability, which are constant over time and in the user’s environment. Temporal metrics represent the characteristics that change over time but are constant in the user’s ecosystem. Environment metrics represent characteristics that are relevant and unique to a specific user.

## 2.4 Upgrades of CVSS4.0

CVSS version 4.0 is a major evolution from version 3.1. Here are some of the most important improvements between the two versions:

Version 4.0 of the Common Vulnerability Scoring System (CVSS 4.0) has been designed with the aim of simplifying the scoring system and making it more accessible to users. This new approach includes improvements in the accuracy of vulnerability assessments, achieved through the introduction of new scoring methods. These methods allow for a more accurate assessment of vulnerabilities, facilitating a clearer and more detailed understanding of the associated risks.

In addition, CVSS 4.0 introduces new metrics, such as Scope and Attack Vector, which provide additional information on the nature of the vulnerability and its impact on the system. A notable improvement in this release is its extended applicability to operational technologies (OT), industrial control systems (ICS) and the internet of things (IoT). Security metrics and values have been integrated into the supplemental and environmental metrics groups, expanding the scope and utility of the tool to assess and mitigate risks in a variety of technology environments (Hispasec, 2023).

## 2.5 Comparison between CVSS4.0 and CVSS3.1

The major difference between CVSS4.0 and CVSS3.1 is the appliance into OT/ICS environments in addition to new nomenclature

* CVSS-B: CVSS Base Score
* CVSS-BT: CVSS Base + Threat Score
* CVSS-BE: CVSS Base + Environmental Score
* CVSS-BTE: CVSS Base + Threat + Environmental Score

Another major difference is when calculating metrics.

While CVS4.0 has 5 types of metrics, CVSS3.1 has only 3 (Base, temporal and environment).

In CVSS4.0 the temporal metric has been eliminated (Ciber 4 All Tarlogic, 2023).

## 2.6 Example of vulnerability measured using CVSS4.0

FIRST provides an online CVSS4.0 calculator to perform the metrics, and also includes a calculator for each CVSSS version. (*Common Vulnerability Scoring System Version 4.0 Calculator*, no date) As an example, a SQL Injection vulnerability affecting an application will be used. This SQL by executing arbitrary code by an unauthenticated user is of critical category, since it affects the server directly (Sysdream, 2017).

Subsequently, the metrics will be analysed with the objective of determining their performance using CVS 4.0, given that the metrics between CVSS versions are different.

The first thing would be to analyze the base metrics of the vulnerability. Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Figure 2 Base metrics (Common Vulnerability Scoring System Version 4.0 Calculator, no date)

**Exploitability metrics:** It refers to the metrics used to measure the vulnerability and exploitability of the exploit itself

**Attack Vector:** Indicates from where the attack has been made, in this case it would be through the network.

**Attack Complexity:** Indicates whether the attack is simple or complex to perform, in this case being a simple SQL injection the complexity is low.

**Attack requirements:** Indicates if any external requirement is needed for the attack to be executed, in this case it is only executed.

**Vulnerable System Impact Metrics:** This metric measures the impact to the vulnerable application.

**Confidentiality:** If it affects the confidentiality of the system, in this case it is high since it executes code in the system.

**Integrity:** If it affects the system itself, in this case it is high because the execution of commands can corrupt the system.

**Availability:** In this case it would be high since the system may result in a service failure.

**Subsequent System Impact Metrics:** This category is new in CVSS 4.0 and measures the consequences of the exploit to the system. It is practically the same effect as in the application.

**Confidentiality:** If it affects the confidentiality of the system, in this case it is high because it executes code in the system.

**Integrity:** If it affects the system itself, in this case it is high since the execution of commands can corrupt the system.

**Availability:** In this case it would be high since the system may result in a service failure.Interfaz de usuario gráfica

Descripción generada automáticamente

Figure 3 Supplemental Metrics (Common Vulnerability Scoring System Version 4.0 Calculator, no date)

**Safety:** When a system does have an intended use or fitness of purpose aligned to safety.

**Automatable:** If the exploit can be automated, even if there is a PoC that PoC is not automatable.

**Recovery:** If the system is resilient to this vulnerability.

**Value Density:** Describe the resources that the attacker Will gain control over with a single exploitation event

**Vulnerability Response Effort:** Provide supplemental information of how difficult it is for consumers to provide an initial response to the impact of vulnerabilities for deployed products and services in their infrastructure

**Provider Urgency:** It signifies the criticality of the vendor to fix this vulnerability.

**Environmental (Modified Base Metrics):** Represents the characteristics of a vulnerability that are relevant and unique to a particular user’s environment.

Considerations include the presence of security controls which may mitigate some or all consequences of a successful attack, and the relative importance of a vulnerable system within a technology infrastructure

Also included are other situation such as:  
Safety and industrial Control Systems (ICS) and Operation Technology (OT)

Imagen que contiene Calendario

Descripción generada automáticamente

Figure 4 Environmental (Modified Base Metrics) (Common Vulnerability Scoring System Version 4.0 Calculator, no date)

In this case, as the vulnerability is not affecting any ICS or OT system, it is not relevant.

**Environmental (Security Requirements):** Represents the characteristics of a vulnerability that are relevant and unique to a particular user’s environment.

Considerations include the presence of security controls which may mitigate some or all consequences of a successful attack, and the relative importance of a vulnerable system within a technology infrastructure

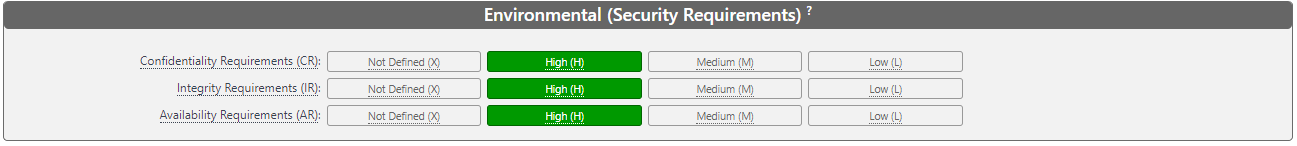


Figure 5 Environmental (Security Metrics) (Common Vulnerability Scoring System Version 4.0 Calculator, no date)

**Confidentiality Requirements:** Should be based on the classification level of the data that is stored or used by the user and applications running on the target system

**Integrity Requirements:** Focus on the importance of the accuracy of the data it stores or uses.

**Availability Requirements:** Should be based on the uptime requirements and redundancy of the device or the applications hosted by the device.

**Threat metrics:** current status of exploit/vulnerability as a threat on the internet

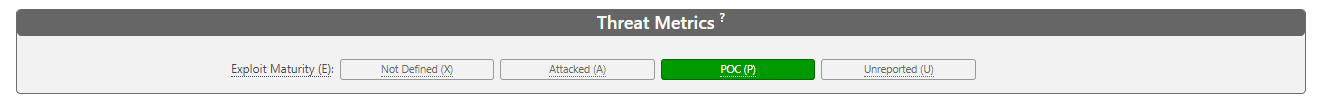


Figure 6 Threat Metrics (Common Vulnerability Scoring System Version 4.0 Calculator, no date)

In this case the PoC metric is granted, as there is a proof of concept published on the internet.

The metric result is classified as high.

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:P/CR:H/IR:H/AR:H/S:P/AU:N/R:I/V:D/U:Red

This is what has to be copied in the report, as CVSS4.0 contains more metrics, the vector is bigger compared to the previous one made in CVSS3.0.

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

(FIRST, 2023).

# 3 Main Chapter

## 3.1 Analysis of PwnDoc

When it comes to reporting, traditionally it was done using a template that the organisation gave to the auditors for certain types of reports, now thanks to tools such as PwnDoc and Docker it is possible to set up centralised applications so that several auditors can work at the same time generating reports.

In this section we will see what PwnDoc is, the features of this software and how to configure it.

## 3.2 What is PwnDoc:

PwnDoc is an automatic pentesting audit report generator, it is open source and is built on Docker and programmed in Python. It is a tool that can be mounted from a central server or independently on workers’ computers for decentralised use, and because it is open source, knowledgeable developers can edit the code to adapt it to the needs of the organisation.

PwnDoc can be used in many areas, for example:

A user who travels a lot and wants to do reporting from the phone.

An organisation that wants to centralise reporting and automate the process.

### 3.2.1 Features of PwnDoc:

PwnDoc is a reporting tool with a number of features that make it easy to use:

* Multi-platform concept: PwnDoc is intended to be mounted on a central server and users connect via the web interface to the server to write reports.
* User accounts: PwnDoc to manage permissions on different reports, implements user accounts to make each user have the necessary permissions to access the resources they request.
* Language generation by language: In PwnDoc you can generate reports in different languages such as English or Spanish.
* Data extraction: PwnDoc can import data from multiple sources, from yaml templates, vulnerability scanners like Nessus or documents.
* Multi-user reporting: PwnDoc has the ability to have multiple users manipulate the report at the same time, similar to Google docs
* Vulnerability management: PwnDoc has a vulnerability library, as an administrator you can add more custom vulnerabilities.
* Reusable data: PwnDoc has the ability to reuse data and vulnerabilities in other audits, as it has a MongoDB database to store that data.
* Vulnerability monitoring: While reporting, you can not only make a custom metric of the vulnerability based on the audit, but you can also monitor whether the vulnerability is reported or not yet finished (Skandashield, 2021).

## 3.3 How to configure PwnDoc:

In order to create configurations, it is first necessary to create an administrator account. This account is of great importance, as it will enable us to control the permissions and users of the application.

Once the initial user has been created, it is necessary to configure the report languages and audit types.Texto

Descripción generada automáticamente

Figure 7 Configuration of languages and audit types (yeln4ts, no-date).

## 3.4 Setting of languages and types of audits

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

Figure 8 List of languages(yeln4ts, no-date).

As PwnDoc is capable of supporting a multitude of languages, it is possible to specify which languages will be used for the reports.

Preview of the application

For all this to work we need to create a template, PwnDoc offers a basic template that can be configured, this template is available on GitHub (yeln4ts, 2022)

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

Figure 9 Template Uploading (yeln4ts, no-date).

To better keep track of clients/organisations, PwnDoc implements a database to store clients and organisations.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Figure 10 Clients database(yeln4ts, no-date).

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Figure 11 Companies Database(yeln4ts, no-date).

Also PwnDoc has the option to create internal users, it also implements an option for the user to be a user of the application, or to have only reporting permissions.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figure 12 Add collaborators(yeln4ts, no-date).

In order to generate a report, three key elements are required:

* Vulnerabilities: PwnDoc needs vulnerabilities to be able to add to the report template.
* Audit Type: PwnDoc needs to know what type of audit is being performed so it can look for the type of vulnerabilities it needs.
* Vulnerability Category: PwnDoc needs to create vulnerability categories to differentiate what type of vulnerabilities they are (yeln4ts, no-date).

To create vulnerability types, go to the Data > Custom Data > Vulnerability Type section.

There will be create vulnerability types.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Figure 13 Creating Vulnerability types(yeln4ts, no-date).

It is necessary to create categories for vulnerabilities. To do so, navigate to Custom Data > Vulnerability Categories.Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Figure 14 Creating Vulnerability Category(yeln4ts, no-date).

This section is useful because in web applications there are different types of vulnerabilities.

Subsequently, the requisite report must be generated. This is accomplished via the Custom Data > Audit Type menu option.Interfaz de usuario gráfica, Aplicación, Correo electrónico

Descripción generada automáticamente

Figure 15 Creating Audit type (yeln4ts, no-date).

It is important to have a loaded template to use it.To create the report go to the Audits section and create a new one, in this case it will be a Web Audit and it will be called “Test Thesis”.Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Figure 16 Creating audit (yeln4ts, no-date).

When we have created the audit, the following window is generated.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

Figure 17 Configuring the new Audit(yeln4ts, no-date).

Here it will have to configure:

* The language
* The template
* The company
* The contributors
* The start date, end date and the day of the audit report
* The scope of the Audit (yeln4ts, no-date)

To add a vulnerability, click on the + button in the Findings section and select a vulnerability from the database.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

Figure 18 Vulnerability selection(yeln4ts, no-date).

After adding them you can edit the description and the impact depending on the scenario, you can also add evidence about the vulnerability and how it can be exploited.Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Figure 19 Proofs Section (yeln4ts, no-date).

The user can also modify the impact of the vulnerability specifically for the report.Interfaz de usuario gráfica, Aplicación, Correo electrónico

Descripción generada automáticamente

Figure 20 Details Section (yeln4ts, no-date).

Once the user added the vulnerabilities in the report, click on download to see the result.

The report that is generated with the default template is quite basic and has some formatting errors and some unnecessary sections.Tabla

Descripción generada automáticamente

Figure 21 XSS vulnerability of the report (yeln4ts, no-date).

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Figure 22 XSS part 2 (yeln4ts, no-date).

But it also has some interesting sections, such as the “Vulnerabilities Summary” section.

Tabla

Descripción generada automáticamente

Figure 23 Vulnerabilities Summary (yeln4ts, no-date).

There is also a General Information section.

Texto, Aplicación

Descripción generada automáticamente

Figure 24 General information (yeln4ts, no-date).

One such section that is not required in the reports is the change history.

Tabla

Descripción generada automáticamente

Figure 25 Modifications history (yeln4ts, no-date).

## 3.5 Limitations of PwnDoc:

After having set up PwnDoc and used it to create a report, the tool has these main limitations:

PwnDoc lacks support for CVSS4.0, which necessitates additional technical knowledge. Additionally, PwnDoc requires a template to be configured for API data display, further demanding technical expertise to create such a template.Tabla

Descripción generada automáticamente

Figure 26 Example of table formatting in report template (yeln4ts, no-date).

## 3.6 Introduction of reporting methodologies:

After having analysed an automatic reporting tool, this time it is time to analyse a handwritten report with the guide proposed by the IEEE, and propose some changes and improvements that can make the reporting phase easier, the purpose of this section is to create a framework where there will not only be recommendations, guidelines and steps on how to make a report, but in the framework will also include a standardisation of the tools that pentesters use on a daily basis, the purpose of this is to standardise the reports and the tools that are used, to create trust between the report, the client and the pentesters, and in turn also to make the reports so that any section of the client company can use this information from a single source.

## 3.7 Phases of a report:

These are the characteristics that a report should have according to IEEE.

1º Executive Summary: This summary is a summary that is normally made to know what has happened, it does not have to have a lot of technical content as it is prepared so that anyone can read it, especially senior managers and CISOs.

2º Project Objective: This section describes the objective of the audit, the scope and the assets to exploit.

3º Timeline: The timeline is a timeline describing the start and end of the audit, as well as important events.

4º Summary of Findings: This section describes the vulnerabilities found and a small proof of concept to replicate them.

5th Summary Of Recommendations: This section makes high level recommendations on how to remediate the vulnerabilities (Alghamdi, 2021).

## 3.8 Contents of a standard report

In this section, we will examine two reports, one from Offensive Security and one from GitHub, in order to gain insight into the main sections of the report and its structure.

Having analysed the recommended parts of a report by the IEEE, will be presented two examples to illustrate the characteristics of each. The first example is a test report produced by a well-known cybersecurity company, Offensive Security.(Offensive Security Services, LLC, 2013).

The second example will be a professional report about a company that has been published (ACK-J, 2023).

It will be analysed using the phases that IEEE has written in their paper (Alghamdi, 2021).

### 3.8.1 1º Executive Summary

Texto, Carta

Descripción generada automáticamente

Figure 27 Offensive Security Executive Summary (Offensive Security Services, LLC, 2013).

The executive summary made by Offensive Security is a bit more general, stating the objectives of the audit and that they comply with the recommendations by NIST SP 800-115.

Texto, Carta

Descripción generada automáticamente

Figure 28 Disclosed Report Executive Summary (ACK-J, 2023).

The executive summary details a project's objectives, findings of critical vulnerabilities, compliance with PCI-DSS and GDPR, the impact of vulnerabilities on the organization, and high-level recommendations for addressing these issues.

### 3.8.2 2º Project Objective

In the Offensive Security report there is no specific Project Objective section, so this section is in the executive summary section.

Texto, Carta

Descripción generada automáticamente

Figure 29 Project Objective of Disclosed report(ACK-J, 2023).

In the GitHub report this is summarised in the Engagement Overview, in this report this section is more extensive, having more useful information such as:

Scope:Tabla

Descripción generada automáticamente

Figure 30 Scope of GitHub disclosed report (ACK-J, 2023).

Methodology:

Diagrama

Descripción generada automáticamente

Figure 31 Methodology of GitHub Report (ACK-J, 2023).

There are also other interesting sections such as “2.3 Technical Impact Metric”, “2.4 Business Impact metric” or “2.5 Mitigation Prioritization Metric”, but these metrics are based on CVSS3.1 will not be highlighted.

### 3.8.3 3º Timeline

In the Offensive Security report there is no timeline.

In the GitHub disclosed report there is a timeline but in the middle of the document.

Tabla

Descripción generada automáticamente

Figure 32 Timeline of disclosed report part 1 (ACK-J, 2023).

Tabla

Descripción generada automáticamente

Figure 33 Timeline of disclosed report part 2 (ACK-J, 2023).

Although the timeline is in the middle of the document, it can be seen that the timeline describes the most notable events in the whole audit process, as well as the start, end and presentation of the audit to the client.

### 3.8.4 4º Summary of findings

Texto, Carta

Descripción generada automáticamente

Figure 34 Summary of findings in Offensive Security Report (Offensive Security Services, LLC, 2013).

In the Offensive Security report the “Summary of findings” section is well summarised, with a brief history of the audit and what has happened at a high level.Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Figure 35 Index of the report (ACK-J, 2023)

In the published GitHub report there are 5 pages dedicated to the summary of the audit, the key findings section is a section that summarises the most salient findings.Texto, Carta

Descripción generada automáticamente

Figure 36 Key findings of GitHub disclosed report (ACK-J, 2023)

The key findings section, however, only describes the most salient findings and does not summarise the audit and the findings that were found, as the Summary of findings has to be a story about what happened in the audit. This section is very long and could be reorganised into other sections, as the purpose of the Summary of findings is to summarise the findings.

Even so, this section has some interesting subsections:

Gráfico, Gráfico circular

Descripción generada automáticamente

Figure 37 Statistics section of GitHub report (ACK-J, 2023)

This section summarises the vulnerabilities found based on web applications

Below is measured based on MITRE ATT&CK’s TTPs, but as this research is focused on web applications this section is not truly relevant.

Gráfico, Gráfico de barras

Descripción generada automáticamente

Figure 38 Vulnerabilities measured by TTPs (ACK-J, 2023)

### 3.8.5 5º Summary of recommendations

Texto, Carta

Descripción generada automáticamente

Figure 39 Summary of recommendations in Offensive Security report (Offensive Security Services, LLC, 2013)

In the Offensive Security report there is a page dedicated to remediation, with a general description of what should be done in the case of maintaining application security.

The 1st part consists of each finding listing remediations at a high level, as in this example:

Texto

Descripción generada automáticamente

Figure 40 Example of mitigation in GitHub disclosed report (ACK-J, 2023)

Texto, Tabla

Descripción generada automáticamente

Figure 41 References of GitHub disclosed report (ACK-J, 2023)

These mitigations are written for general purpose, and are at a high level, referencing a standard to make them understandable.

It also includes a reference section to make it more helpful.

### 3.8.6 6º Example of a description of findings:

In the reports there are 2 ways to describe the findings in a report

* History: This way is focused on audits where a real objective is planned, like getting Domain Admin, Remote Code Execution or a company imposed objective, the benefit of this way of reporting is to see in a simple way how the application can be exploited, but a disadvantage is that the vulnerabilities cannot be categorised by criticality, making it a bit more complicated to see the remediation of the vulnerabilities.
* Individually: When it is in the context of a web application or an application itself, vulnerabilities can be reported individually categorised by criticality, this could be useful for example if the company has not set a goal to get any accounts or access.

The Offensive Security report lists the findings in an orderly fashion using a narrative.

Texto

Descripción generada automáticamente con confianza media

Figure 42 “Attack Narrative” Index in Offensive Security Disclosed report (Offensive Security Services, LLC, 2013)

An example of how a vulnerability is reported in this format would be the following:

Interfaz de usuario gráfica, Texto, Sitio web

Descripción generada automáticamente

Figure 43 Example of narrative reporting in Offensive Security Report (Offensive Security Services, LLC, 2013)

In the context of the report, what has happened is that an exploit is being used to access a system shell with credentials, highlighting the domain and a picture as proof of concept.

The GitHub report is different. Firstly the vulnerabilities are reported according to their criticality, secondly the information is more organised and in sections.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figure 44 Organization of findings in GitHub disclosed report (ACK-J, 2023)

It is organised in such a way that thanks to the colours and numbers you can see the criticality of the vulnerability, also the victim, the impact this vulnerability has on the GDPR, details on how it was discovered and some additional information.

In addition, for each vulnerability there is a section on how to replicate the vulnerability.Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figure 45 Replication section of GitHub disclosed report (ACK-J, 2023)

And a section on vulnerability-related mitigations.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Figure 46 Mitigation and references of GitHub Disclosed report (ACK-J, 2023)

## 3.9 Proposal of the standard with improvements

After having compared 2 styles of professional reports, new ideas will be proposed to add to the reporting process, all these ideas have been thought so that they do not modify or alter to a great extent, the report structure and the sections of the report.

Table 1 Report Improvements

|  |
| --- |
| Video timeline of the whole assessment: If the audit is a network team exercise focused on objectives, a walkthrough can be made until the objective is reached by exploiting the vulnerabilities, and in table format (see figures 34 and 35) |
| Video exploiting the vulnerability: If the report is an audit of a web application a video exploiting each vulnerability in addition to the proof of concept. |
| Report in markdown format: An additional report in markdown format for data parsing including the additional videos. |
| Section of the exploits used in the audit: A section in the document of the exploits used. |
| Standardise audit tools and how to introduce new tools: In the report and in this standard, establish a set of highly used tools that are used on a daily basis and have a section in the report where the tools used in this audit are listed. |
| Inclusion of used wordlists: A section in the document with the used wordlists. |
| Reorganisation of vulnerabilities in the report: Write 2 sections, in case of narrative report make an additional section with each vulnerability detailed. |
| Inclusion of CVSS4.0 reports: CVSS4.0 reports. |
| Use timeline and report and Retest: Do a final test using the report and video to verify if the route can be exploited. |
| Bar chart with metrics of vulnerabilities found OWASP TOP 10: A graph based on the OWASP tops categorizing the vulnerabilities that have been found. |
| Table with remediation importance in reports: Section with remediation priority in reports. |
| Table with vulnerability complexity in reports: Section with exploit complexity in report |

## 3.10 Example of a report with proposed improvements

Next, the organisation of the new report will be done, with the new sections and what will be in each one. This will be used as a demo and then shared with the 5 security professionals who will be in charge of evaluating this new standard. The Markdown report will follow the same standards but done in markdown.

Table 2 Example of report

|  |
| --- |
| EXAMPLE OF REPORT |
| 1º Table of Contents: A table of contents with all the sections of the report. |
| 2º Index of figures: An index with all the images of the report. |
| 3º Table of contents: A table of contents with all the tables in the report |
| 4º Executive summary:  A summary of 3 paragraphs. The first paragraph will be a summary of the dates the report occurred, the second paragraph will be a high level summary of what happened in the audit, and the third paragraph will be a summary of the criticality of the vulnerabilities found. |
| 5º OWASP Top 10 Summary:  A bar chart or pie chart with each OWASP top and the number of vulnerabilities that have appeared in each top. |
| 6º Vulnerability remediation table:  A table with the urgency of remediation of all vulnerabilities. |
| 7º Vulnerability complexity table:  A table with the complexity of all vulnerabilities. |
| 8º Tools used:  A section with the tools used in the audit, organised by their use:   * Enumeration tools * Exploitation tools * Post-Exploitation tools |
| 9º Timeline:  The timeline will be in video format and in table format, in table format will include the important events of the audit (administrator access, exploit discovered). if the audit has an objective it will be done in that format, otherwise the following format will be used:  Table with:   * Start of audit * End of audit * Day of the report |
| 10º Vulnerability analysis:  This section will detail the vulnerabilities found, it can be detailed in 2 methods  Narrative: If the audit has a target (administrator, command execution) it will be explained telling how it has been exploited, from the enumeration to the administrator.  Individual: If the audit is carried out on individual targets such as applications, vulnerabilities will be reported in order of their criticality. |
| 11º Exploits Used:  A table with the exploits that have been used and where they have been used. |
| 12º Wordlist used:  A table with the wordlist used in each tool. |

## 3.11 Professional Survey

### 3.11.1 Survey objective and questions

The objective of this survey is to evaluate the implementation of a CVSS4.0 report, and to assess the possible standardisation of the report in penetration testing across all companies.

There are a total of ten questions in the questionnaire, four of them are development questions that ask the practitioner to give an opinion on various points such as the difference in their company's reporting, some positive and negative aspects of the report, or possible improvements of this system. These development questions help the research to receive an open point of view from the respondent.

In addition there are six questions with limited answers to Yes/No Agree/Disagree, these questions help to find out in a more direct way certain important aspects of the report such as regulatory compliance, compliance with corporate requirements and an open question whether it is possible from the interviewee's point of view to implement the report in her/his company(Appendix J).

The aim of this survey is that 5 professionals in the cybersecurity sector, analyse the proposed report, creating it and comparing it with the report that they make in their company when making a penetration testing, through the survey, the 2 reports will be analysed and compared and the questions will be answered, then with the answers collected a critical analysis of the answers will be made and some objectives of improvement of the report will be proposed, and based on the answers, generate a general conclusion of the viability of the report in the organisations.(Dworkin, 2012).

# 4 Legal Considerations

Implementing a standardised reporting framework for penetration testing using CVSS 4.0 in the UK involves several key legal considerations. Compliance with the Data Protection Act 2018 and GDPR is paramount, requiring strict protocols for handling sensitive data. Explicit consent must be documented from all parties involved, including the commissioning organisation and any affected third parties, detailing the scope, objectives and potential risks of testing.

The use of pentesting tools and techniques must comply with the Computer Misuse Act 1990 to avoid unauthorised access and its serious legal consequences. In addition, adherence to industry standards, such as the National Cyber Security Centre (NCSC) guidelines and ISO/IEC 27001, is crucial to ensure that methodologies are ethical and accepted worldwide.

Confidentiality and integrity in the handling of findings and reports are critical. Vulnerabilities must be carefully disclosed to avoid exploitation by malicious actors, and non-disclosure agreements (NDAs) must be in place to protect sensitive information(*Legal aspects in research*, no date).

# 5 Ethical Considerations

Ethical Considerations

Implementing a standardized reporting framework for penetration testing using CVSS 4.0 in the United Kingdom involves significant ethical considerations. Ensuring the privacy and confidentiality of all data involved in the pentesting process is paramount. This includes not only protecting the data of the organization commissioning the pentest but also any third parties whose data may be accessed. Ethical guidelines mandate that sensitive information should only be used for the intended purpose and should be anonymized wherever possible to prevent misuse.

Consent is another crucial ethical aspect. All parties involved must be fully informed about the scope, objectives, and potential risks of the pentest. Obtaining informed consent ensures that all stakeholders are aware of and agree to the testing procedures, thereby respecting their autonomy.

Transparency and honesty in reporting are essential. Findings must be presented accurately and objectively, without exaggeration or understatement, to provide a true reflection of the security posture. Additionally, the responsible disclosure of vulnerabilities is vital. This means communicating findings to the affected parties promptly and providing them with sufficient information to address the issues without exposing them to further risk.

Moreover, ethical conduct requires adherence to professional standards and guidelines, such as those provided by the National Cyber Security Centre (NCSC) and other relevant bodies. Maintaining integrity, accountability, and fairness throughout the pentesting process ensures that ethical standards are upheld, fostering trust and credibility in the cybersecurity field(*Ethics in research*, no date).

# 6 Methodology /Methods

A quantitative approach has been chosen to assess whether report writing and structuring contribute to improved decision-making.

The population of interest comprises professionals in the offensive security sector. To represent this population, a survey sample was selected from a group of 5 professionals, who were interviewed with specialised questions.

The data used in this study comes primarily from sources such as IEEE Research, organisational blogs and organisational newsletters. These sources provide a variety of perspectives and relevant information on the relationship between reporting and decision making.

Surveys were distributed to a representative group of randomly selected professionals. Clear information on the purpose of the study was provided and the confidentiality of responses was guaranteed. A time limit was set for data collection, after which the analysis proceeded.

The advantages of using this methodology are:

1º The quality of the participants’ responses

2º A more objective analysis can be carried out.

The disadvantages of using this methodology are:

1º The response time of the interviewees

2º To be more precise, the study must be carried out with more participants.

# 7 Findings

### 7.1Automatic Vs Manual reporting

Prior to undertaking a comparison of different reporting methods, it is essential to first establish a set of criteria by which the effort involved in setting up the infrastructure and generating the report can be deemed "easy." This discussion is particularly pertinent when considering manual reporting, which typically involves the utilisation of a template created in Google Docs or Word.

1. Time Efficiency: The task should be quick to perform, requiring no significant investment of working hours. It should fit within the normal workflow without necessitating overtime or extra effort.

2. Simplicity: The process should not require advanced skills or experience. Ideally, it should be manageable with basic skills common in the field, or even by someone new with minimal guidance. The task should be straightforward, allowing easy inclusion of custom tables and fields into standard report templates.

3. Adaptability: Updating the report to incorporate new technologies (such as metric tools, videos, etc.) should be straightforward.

With these criteria in mind, we aim to identify a system that aligns closely with these standards:

1. Efficient Workflow: The reporting process should not exceed one normal working day. Thanks to efficient infrastructure, it should allow quick access to necessary data (e.g., client details, vulnerabilities).

2. Customizability: Customizing the report template by adding sections, content fields, and tables should be simple and not require additional technical skills.

3. Future-proof Infrastructure: The infrastructure should accommodate new technologies or metrics (like adding a CVSS 4.0 calculator or integrating videos and dynamic content) effortlessly. Additionally, it should not require extra knowledge or effort from an auditor to incorporate new metrics or multimedia systems when updating the infrastructure or modifying templates(Siegrist *et al.*, 2004).

Table comparing manual and automatic reporting.

|  |  |  |
| --- | --- | --- |
|  | Manual | Automatic |
| Time | The time effort is significant, it requires an investment of time to calculate vulnerabilities, search for data related to vulnerabilities, evidence, description of vulnerabilities, any external information has to be searched on the internet and that is time consuming. | The time effort required is less than manual reporting, because PwnDoc has a centralised DDBB with vulnerabilities, it is easier to access the data, the information you need is centralised and because the report creation is automated, you would only need to modify the bugs.(yeln4ts, no date b) |
| Skill | No additional technical knowledge is required to add customised content to the report, it is as simple as inserting into the report | It requires additional technical knowledge to manipulate the default PwnDoc template and add custom content, plus it requires extra effort to manipulate the data and the api to make the content fit the field.(yeln4ts, no date) |
| Adaptation | As it is a text document template, it is very easy to add multimedia content (videos, recordings, photography). | Requires additional technical knowledge to add multimedia content (videos, animations) to the report, and technical capacity to modify the infrastructure. (yeln4ts, no date) |

Table 1 Criteria Comparison

Automatic reporting saves time, but as manual reporting is very versatile and does not require additional technical knowledge to add customised content, it is the most suitable method to be used in conjunction with the proposed report in the standard.

The most viable reporting system to use in conjunction with the proposed report is manual reporting, as manual reporting is more adaptable, does not rely on additional expertise, and can support new technologies such as multimedia content (videos, images, graphics).

### 7.2 Report Writing

Comparison of reporting methods

To compare reporting methods, these criteria will be used to determine which type of reporting is most appropriate, based on the SANS standard:

Detail: That the content of the sections recommended by SANS meets the description of that section.

Content: That the report complies with the sections recommended by SANS, both SANS and IEEE recommend certain sections in the reports, the more sections there are in the report, the more likely it is to be adapted.

Innovation: That there are extra sections that include new content and that there is no content that is repeated from other sections. Having innovative sections (summary sections with graphs, tables etc) helps to understand in detail the report and eliminate the impact of vulnerabilities, and also add more context to the report (Mansour A, 2010).

Table 3 Comparison of reporting methods

|  |  |  |
| --- | --- | --- |
|  | GitHub style report | Offensive Security Style report |
| Detail | The GitHub style report meets the minimum requirements that the description of the SANS report sections explains. In the findings section, the GitHub report does not do the NIST-based risk evaluation.(Mansour A, 2010). | The Offensive Security style report meets the minimum requirements of the SANS report section descriptions, although the report has few sections and sections such as Executive summary (from the Offensive Security report) combine content with Scope of work (SANS report), making it difficult to understand the text.(Mansour A, 2010). |
| Content | The report complies with most of the key sections of the report, these sections are missing:  Planning  Exploitation  Reporting  The sections that the report complies with are unordered, but are coherent with each other, making the report by numbering guide the reader to see the key sections.(Mansour A, 2010). | Most of the key sections are included in the report, but because they are mixed together they make it difficult for the non-technical reader to understand, these are the sections that the report does not have:  Assumption  Timeline  Methodology  Planning  Exploitation  Reporting  The overall structure of the report is a structure that is focused on narrative reporting.(Mansour A, 2010) |
| Innovation | The GitHub report includes new sections to make the report clearer:  Key findings: The key findings that require the most attention because of context or severity.  Key remediations: The remediations that most urgently need to be patched.  Technical Impact metric: A table of criticality based on your CVSS 3.1 score.  Business impact metric: Overall risk to the target organisation, its impact and likelihood.  Mitigation prioritization metric: Table explaining the different categories of criticality.  Tools: the tools that have been used  Response plan: In this section, based on the categories the vulnerabilities are organised based on the urgency to remediate them.  Assessment Artifacts: The temporary artifacts that have been created for testing on the target (test DDBB with name ‘test1’). | The report proposed by Offensive security has interesting sections:  Conclusion: a final summary of whether the objectives of the exercise have been achieved. |

The reporting method that would best suit the proposed report is the GitHub report.

* It meets most of the key sections proposed by SANS.
* The report is organised and structured, with separate sections to explain specific documentation, making it more understandable and clearer for all audiences.
* Meets the minimum content requirements of the SANS sections, making it very compatible with the requirements imposed by any company.
* Provides depth on how vulnerabilities are exploited, the report being of individual type, makes it more in depth in the details of the exploitation of vulnerabilities.

Survey Feedback

After having analysed the responses, several general points have emerged

General Points:

* The report meets the reporting requirements of the organisations, with an 80% response of ‘Yes’, and a 20% response of ‘I don't know’.

Gráfico, Gráfico circular

Descripción generada automáticamente

Figure 47 Question 2

- The report meets the reporting requirements of the organisations, with 80% affirmative responses and 20% negative responses.Gráfico, Gráfico circular

Descripción generada automáticamente

Figure 48 Question 4

* 60% of respondents consider that the proposed report has more sections than their organisation's report, while 40% say it does not.Gráfico, Gráfico circular

  Descripción generada automáticamente

Figure 49 Question 6

* All respondents felt that their supervisor would approve of the implementation of the reporting method, 60% agreed, and 40% strongly agreed.Gráfico, Gráfico circular

  Descripción generada automáticamente

Figure 50 Question 8

* The report complies with current standards such as NIST in 2 organisations out of 5 (40%), on the other hand in 2 organisations out of 5 it is not known whether it complies or not (40%), and in 1 organisation out of 5 it does not comply with the standards (20%).Gráfico, Gráfico circular

  Descripción generada automáticamente

Figure 51 Question 9

* 60% think that the report is not long to read, but 40% strongly think it Gráfico, Gráfico circular

  Descripción generada automáticamente

Figure 52 Question 10

Analysing these general points together with the 4 freely developed questions that were asked, the following conclusions have been reached.

Table 4 Positive and negative aspects of the report

|  |  |
| --- | --- |
| Positive | Negative |
| promoting accountability, transparency, and providing a mechanism for addressing issues | potential abuse, false reports, and increased workload for moderators or administrators |
| Simplicity, thoroughness, clarity | Very detailed, with sections that are probably unnecessary, No discussion of the reputational and financial impact on organisations. |
| Detailed report | Depending on the nature of the report, if it is technical or executive, the sections Tools Used, Exploit used and Wordlist used are unnecessary. |
| Clear and detailed report, making it understandable for both technical and non-technical people. | N/A |

The report is clear and detailed, so that both technical and non-technical audiences can understand it; however, its detail makes it lengthy and some companies discard certain sections as unnecessary information. The interviewees‘ reports are quite similar, differing only in the order of the sections or in some customised sections missing from the proposed report, which, together with the interviewees’ consideration that it could be standardised for the sector, makes the report adaptable and compliant with current company and global regulations such as NIST or ISO7001. In addition, this report is easy to replicate due to its similarity in length and content to other companies‘ reports, and although it contains more sections than some of the interviewees’ company reports, no additional effort is required to write it.

The interviewees answered all the questions, they have proposed certain improvements to the report,

* “Systemic issues (issues that are noticed many times during the pentest, such as outdated software, or lack of encryption on web traffic), as well as a section on impact to the client.”
* “I propose to make it shorter and more concise”
* “The scope of the audit, the scope of scope of the audit, scope of testing.”

# 8 Evaluation

It has not been possible to answer the research hypothesis, as the research gave results that were not sufficient to answer the hypothesis. Only 1 research question could be answered, related to how the reporting process could be standardised, in this case, giving positive results from the survey and the participants' responses. There are other questions that have been partially answered, it has been possible to show how a metric looks like in CVSS4.0, but it has not been possible to show by means of a demo how it would look like implemented in a report.

In conclusion, the research has not been able to fully answer both the hypothesis and the research questions, but it has yielded relevant information from the sector, such as that reports must have an adequate quality between detail and content to be understandable by all audiences, using as a guide the SANS and IEEE papers and also using sections of reports from independent professionals can achieve a balance between clarity and content suitable for all audiences (Appendix K).

# 9 Discussion

## 9.1 Evaluation of the literature

The literature review in this research addressed two key elements: OWASP and CVSS. OWASP helped to understand how various vulnerabilities impact web applications, while CVSS allowed for analysis and comparison of vulnerabilities with previous versions. Although this section provided a theoretical basis for the study, which focused on the analysis of web application reports according to new standards, it was not crucial for the final results, which differed from the initial hypothesis. The main limitations were the research time and the sources used. Satisfactory results were achieved, but a focus on data analysis techniques could have better supported the hypothesis by linking decisions and cyber-attacks in companies.

## 9.2Assessment of the methodology

In the discussion section of the thesis, the methodology employed revealed strengths such as the use of high quality sources and the guarantee of confidentiality, which promotes data integrity. However, the limited sample size and the collection of data through surveys posed significant challenges. Increasing the sample would be critical to strengthen the generalisability of the results. Furthermore, incorporating additional data collection methods, such as document analysis, and the application of more sophisticated statistical techniques could deepen the understanding of the influence of report writing on decision-making, resulting in more robust research applicable to the field of offensive security.

## 9.3Evaluation of the main key findings

### 9.3.1Manual vs. automated reporting

A critical facet of the research involved comparing two types of reporting infrastructures and assessing which was more effective. A positive aspect of this approach was the inclusion of multiple dimensions associated with reporting, which increased the relevance of the analysis. However, the study was focused in such a way that it only partially answered one of the key research questions: the comprehensibility of automatic reporting infrastructures. It would have benefited from a more thorough examination of the infrastructure, drawing on previous studies of similar reporting systems. In addition, the research could have explored other aspects relevant to the implementation of these infrastructures, such as costs, training requirements and performance.

### 9.3.2Reporting methods

The study examined various reporting methodologies, relying on two primary sources: a report from a recognised company and one that has been disclosed to the public. It is crucial to analyse reports from established companies, as these tend to adhere to standards set by both regulatory organisations and existing regulations. In addition, the assessment of a public report offers an alternative perspective on reporting methodology.

However, this section of the analysis could have been enriched by including a larger number of reports from a variety of leading cybersecurity organisations as well as prominent industry figures. The limited sample of only two reports restricted the depth and quality of the analysis. A larger corpus of documents would have facilitated a more robust and potentially more illustrative assessment in order to propose a standardised and optimised report format.

### 9.3.4 Survey

The survey administered to participants yielded results that are considered satisfactory for the research, highlighting the compatibility and performance of the reporting system from the perspective of industry practitioners, with highly favourable findings for the study and validating the feasibility of implementing this system in contemporary companies. However, due to time constraints, the small number of participants and the paucity of questions, the results obtained lack the necessary depth to make the report robust enough to be considered a standard.

To improve the quality and scope of the research, it would have been prudent to implement more rigorous selection criteria for participants, including not only technical professionals but also individuals in managerial and analytical positions. In addition, the survey questions could have focused more specifically on reporting infrastructures. Providing participants with a concrete example of the type of reporting to be evaluated would have allowed for a more detailed and contextualised analysis of its effectiveness and applicability.

## 9.4 Results

The results obtained from the research have been largely satisfactory. It has been found that the report designed is highly compatible with contemporary organisations. In addition, it was found that infrastructures exert a significant influence on the performance of professionals when writing reports, affecting the effort required and the personalisation of the reports.

Although the research questions and hypothesis were partially answered, the data collected were insufficient to fully validate these propositions. To strengthen the findings, a more rigorous approach could have been implemented in the selection of the research analysed and the methodologies employed, such as data analysis or advanced statistical techniques. In addition, conducting a more diverse and inclusive survey would have enhanced the representativeness and relevance of the results, providing a stronger basis for the confirmation or refutation of the hypothesis and research questions formulated.

# 10 Conclusion

This research was conducted in order to identify, through the creation of a detailed report using the new CVSS4.0 standard, whether corporate cybersecurity reports affect decision making in companies, thus avoiding catastrophes such as attacks or saving costs, based on a quantitative analysis and by conducting a survey of professionals to see the effectiveness of the report. Based on the responses and the analysis of the different methodologies, it can be concluded that the order, the detail in the sections and the content of the sections affect the understanding of the report by different audiences (technical and non-technical), and it has also been found that companies do not faithfully follow the standards proposed by IEEE and SANS.

In this research we have learned how to calculate vulnerabilities with CVSS4.0, how to use the PwnDoc infrastructure and how to conduct effective surveys to get the required data. With all the knowledge acquired and referenced in this research, a researcher can use the content of this paper to learn how to perform metrics with CVSS 4.0, or install an automatic reporting infrastructure such as PwnDoc.

This research illustrates that reporting has to be of a standard of detail, clarity and length, and that it has to be just right as the reader may lose track of what has been discovered. The question also arises as to whether a reporting template can be standardised across the sector, as corporate requirements for companies to require a minimum of content in their reports make standardising a system difficult.

Based on these findings, researchers should make surveys more inclusive, including management and analytical positions in the surveys, also increase the number of reports analysed and conduct more tests and create test reports from the samples.

# References

ACK-J (2023) *Public pentest Report*, *GitHub*. Available at: https://github.com/juliocesarfort/public-pentesting-reports/blob/master/CPTC/2021/finals-c.pdf (Accessed: 7 May 2024).

Alghamdi, A. (2021) ‘Effective Penetration Testing Report Writing | IEEE Conference Publication | IEEE Xplore’, in. Available at: https://ieeexplore.ieee.org/abstract/document/9591097 (Accessed: 2 March 2024).

Ciber 4 All Tarlogic (2023) *CVSS v4: Evaluar las vulnerabilidades para priorizar su mitigación*, *Tarlogic Security*. Available at: https://www.tarlogic.com/es/blog/cvss-v4/ (Accessed: 2 March 2024).

*Common Vulnerability Scoring System Version 4.0 Calculator* (no date) *FIRST — Forum of Incident Response and Security Teams*. Available at: https://www.first.org/cvss/calculator/4.0 (Accessed: 7 May 2024).

Dworkin, S.L. (2012) ‘Sample Size Policy for Qualitative Studies Using In-Depth Interviews’, *Archives of Sexual Behavior*, 41(6), pp. 1319–1320. Available at: https://doi.org/10.1007/s10508-012-0016-6.

*Ethics in research* (no date). Available at: https://www.aurora.umu.se/en/education-and-research/support-for-research/research-planning/ethics-in-research/ (Accessed: 9 May 2024).

FIRST (2023) *CVSS v4.0 User Guide*. Available at: https://www.first.org/cvss/v4.0/user-guide (Accessed: 2 March 2024).

Hispasec (2023) *CVSS 4.0: Nueva versión de evaluación de vulnerabilidades - Una al Día*. Available at: https://unaaldia.hispasec.com/2023/11/cvss-4-0-nueva-version-de-evaluacion-de-vulnerabilidades.html (Accessed: 2 March 2024).

*Legal aspects in research* (no date). Available at: https://www.aurora.umu.se/en/education-and-research/support-for-research/research-planning/legal-aspects-in-research/ (Accessed: 9 May 2024).

Mansour A (2010) *Write a penetration testing report*, *Egnyte*. Available at: https://sansorg.egnyte.com/dl/yNfjHOQix8 (Accessed: 18 April 2024).

Offensive Security Services, LLC (2013) ‘Penetration Test Report’. Available at: https://www.offsec.com/reports/sample-penetration-testing-report.pdf (Accessed: 28 February 2024).

OWASP (no-datea) *A01 Broken Access Control - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A01\_2021-Broken\_Access\_Control/ (Accessed: 2 November 2023).

OWASP (no-dateb) *A02 Cryptographic Failures - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A02\_2021-Cryptographic\_Failures/ (Accessed: 2 March 2024).

OWASP (no-datec) *A03 Injection - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A03\_2021-Injection/ (Accessed: 2 March 2024).

OWASP (no-dated) *A04 Insecure Design - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A04\_2021-Insecure\_Design/ (Accessed: 2 March 2024).

OWASP (no-datee) *A05 Security Misconfiguration - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A05\_2021-Security\_Misconfiguration/ (Accessed: 2 March 2024).

OWASP (no-datef) *A06 Vulnerable and Outdated Components - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A06\_2021-Vulnerable\_and\_Outdated\_Components/ (Accessed: 2 March 2024).

OWASP (no-dateg) *A07 Identification and Authentication Failures - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A07\_2021-Identification\_and\_Authentication\_Failures/ (Accessed: 2 March 2024).

OWASP (no-dateh) *A08 Software and Data Integrity Failures - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A08\_2021-Software\_and\_Data\_Integrity\_Failures/ (Accessed: 2 March 2024).

OWASP (no-datei) *A09 Security Logging and Monitoring Failures - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A09\_2021-Security\_Logging\_and\_Monitoring\_Failures/ (Accessed: 2 March 2024).

OWASP (no-datej) *A10 Server Side Request Forgery (SSRF) - OWASP Top 10:2021*. Available at: https://owasp.org/Top10/A10\_2021-Server-Side\_Request\_Forgery\_%28SSRF%29/ (Accessed: 2 March 2024).

OWASP (no-datek) *OWASP Top Ten | OWASP Foundation*. Available at: https://owasp.org/www-project-top-ten/ (Accessed: 2 March 2024).

PortSwigger (no-date) *Insecure direct object references (IDOR) | Web Security Academy*. Available at: https://portswigger.net/web-security/access-control/idor (Accessed: 2 March 2024).

Redaccion (2023) *La mala comunicación entre los directivos y sus equipos es principal motivo de ciberincidentes en el 65% de las empresas*, *RRHH Digital*. Available at: https://www.rrhhdigital.com/secciones/tecnologia-e-innovacion/156335/La-mala-comunicacion-entre-los-directivos-y-sus-equipos-es-principal-motivo-de-ciberincidentes-en-el-65-de-las-empresas/ (Accessed: 7 May 2024).

Siegrist, J. *et al.* (2004) ‘The measurement of effort–reward imbalance at work: European comparisons’, *Social Science & Medicine*, 58(8), pp. 1483–1499. Available at: https://doi.org/10.1016/S0277-9536(03)00351-4.

Skandashield (2021) *PWNDOC — COMPLETE GUIDE | by Skandashield | Medium*. Available at: https://skandashiled.medium.com/pwndoc-complete-guide-b927956d06d5 (Accessed: 2 December 2023).

Sysdream (2017) *phpCollab 2.5.1 - SQL Injection*, *Exploit Database*. Available at: https://www.exploit-db.com/exploits/42935 (Accessed: 7 May 2024).

yeln4ts (2022) *pwndoc/backend/report-templates/Default Template.docx at main · pwndoc/pwndoc*, *GitHub*. Available at: https://github.com/pwndoc/pwndoc/blob/main/backend/report-templates/Default%20Template.docx (Accessed: 7 May 2024).

yeln4ts (no-datea) *Audits*. Available at: https://pwndoc.github.io/pwndoc/#/audits (Accessed: 2 March 2024).

yeln4ts (no-dateb) *Data*. Available at: https://pwndoc.github.io/pwndoc/#/data (Accessed: 2 March 2024).

yeln4ts (no date a) *Docx Template*. Available at: https://pwndoc.github.io/pwndoc/#/docxtemplate (Accessed: 9 April 2024).

yeln4ts (no date b) *Features*. Available at: https://pwndoc.github.io/pwndoc/#/ (Accessed: 9 April 2024).

yeln4ts (no-datec) *Vulnerabilities*. Available at: https://pwndoc.github.io/pwndoc/#/vulnerabilities (Accessed: 2 March 2024).

# Appendices

## Appendix B: Marking Scheme

The researcher accepts the use of the standard marking scheme.

## Appendix C: Changes to research proposal

## The focus of the research was changed, originally it was going to investigate the implementation of AI Prompts, in the research this part of the research has been eliminated.

## Appendix D: Project Management

Gantt Chart

Gráfico, Gráfico de cajas y bigotes

Descripción generada automáticamente

Figure 53 Gantt Chart

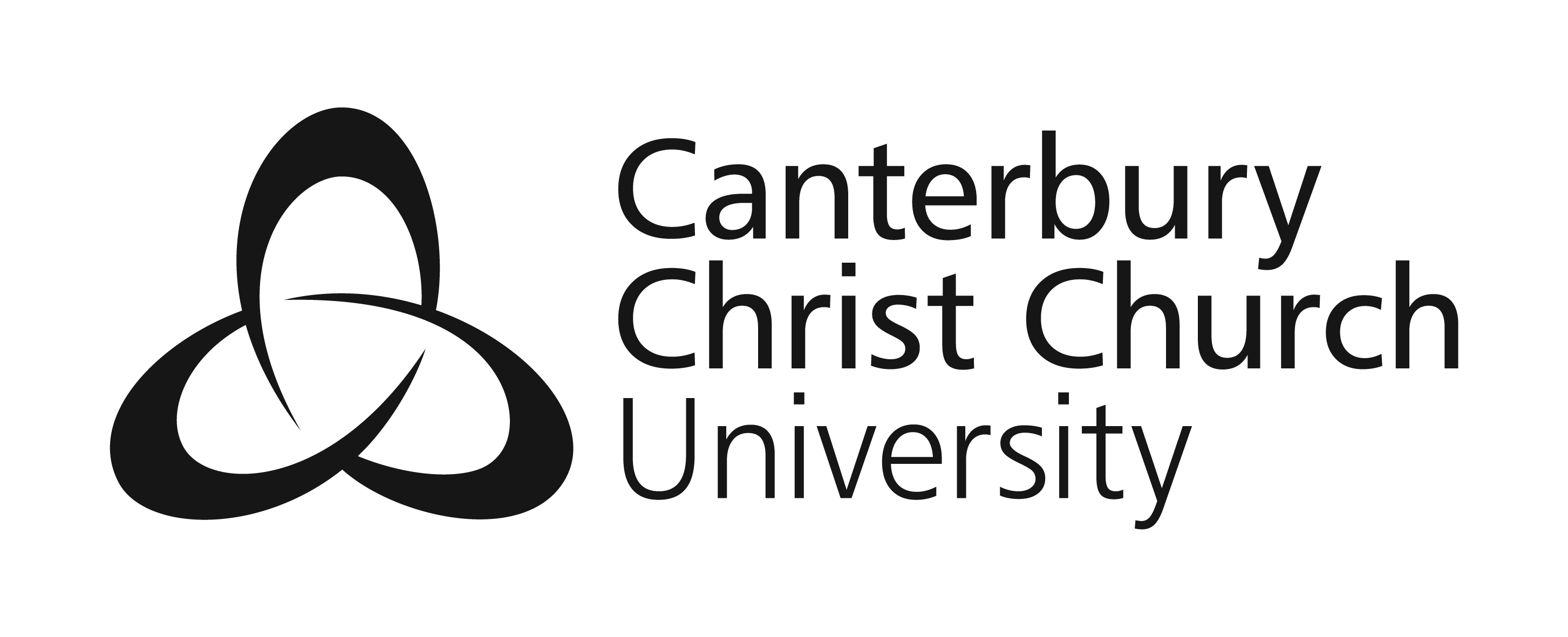
## Appendix E: Meetings With supervisor

|  |  |
| --- | --- |
| Date and location | Purpose |
| 15/02/2024 – Online via Microsoft Teams | Thesis Feedback |
| 20/03/2024 – Online via Microsoft Teams | Methodology, Findings and Disscussion |

## Appendix F: Survey Questionnaire

|  |  |
| --- | --- |
| Do you consent to use the answers to the research questions? No personal data will be requested, only the  answers and the questions. For more information, check <https://www.canterbury.ac.uk/services/governance-and-legal-services/data-protection/privacy-notices/student-privacy-notice> | * Yes * No |
| In your opinion, what are the positive and negative aspects of the proposed report system? |  |
| The proposed report complies with the reporting requirements imposed by the organisation. | * Yes * No |
| How does the propose reporting system differ from your company reporting system? |  |
| Do you consider that the proposed report could be a standard in the sector? | * Strongly Agree * Agree * Disagree * Strongly Disagree |
| In your opinion has it been difficult to create a report with the proposed report system? why? |  |
| Does the proposed report have more sections than your organisation's report? | * Yes * No * I don’t know |
| what aspects of the proposed report would you improve? |  |
| Do you think your supervisors would approve the implementation of the proposed report? | * Strongly Agree * Agree * Disagree * Strongly Disagree |
| The proposed report complies with current standards (NIST, ISO27001). | * Yes * No * I don’t know |
| Do you find the report long to read? | * Strongly Agree * Agree * Disagree * Strongly Disagree |

## Appendix G: Participant Information Sheet:

****

Evaluation of penetration testing reporting methods using CVSS4.0

**PARTICIPANT INFORMATION**

A research study is being conducted at Canterbury Christ Church University (CCCU) by *Marco Carrasco*

Please refer to our [Research Privacy Notice](https://www.canterbury.ac.uk/university-solicitors-office/data-protection/privacy-notices/privacy-notices.aspx) for more information on how we will use and store your personal data*.*

**Background**

*This survey is part of a research project on the analysis of current reporting methods and the*

*current reporting methods, and the creation of a new reporting standard using the new CVSS4.0*

*reporting standard using the new CVSS4.0 metrics system.*

**What will you be required to do?**

Participants in this study will be required to *create a report using the structure of the proposed report, they usually write in their organisation, compare the characteristics of each report, and evaluate it using the questions.*

**To participate in this research you must:**

*Be a cybersecurity professional, with at least 1 year working / bug bounty experience, or in a similar management position, with certifications, or active in ethical hacking communities.*

**Procedures**

You will be asked to *create a report based on the proposed report, participate in a questionnaire and answer questions about the proposed report.*

**Feedback**

*No feedback will be provided, only the answers will be used in the thesis, if the participant asks, a copy of the thesis will be available for download.*

**Confidentiality and Data Protection**

The following categories of personal data (as defined by the [General Data Protection Regulation](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/) (GDPR)) will be processed:

* *No personal data is requested, nor processed. Non-personal data is used solely for the purpose of this research.*

We have identified that the public interest in processing the personal data is:

* *No personal data is requested, nor processed. Non-personal data is used solely for the purpose of this research.*

Data can only be accessed by, or shared with:

* *The researcher and the supervisor*.

The identified period for the retention of personal data for this project:

* *From 22/03/2024 to 01/05/2024* .

If you would like to obtain further information related to how your personal data is processed for this project please contact *Marco, mc1381@cantebury.ac.uk*.

You can read further information regarding how the University processes your personal data for research purposes at the following link: Research Privacy Notice - <https://www.canterbury.ac.uk/university-solicitors-office/data-protection/privacy-notices/privacy-notices.aspx>

**Dissemination of results**

*The results will be published in the research*

**Process for withdrawing consent to participate**

You are free to withdraw your consent to participate in this research project at any time without having to give a reason. To do this *send an email to* [*mc1381@canterbury.ac.uk*](mailto:mc1381@canterbury.ac.uk) *if you want to withdraw from the survey.*

You may read further information on your rights relating to your personal data at the following link: Research Privacy Notice - <https://www.canterbury.ac.uk/university-solicitors-office/data-protection/privacy-notices/privacy-notices.aspx>

**Any questions?**

Please contact *Marco* on*mc1381@canterbury.ac.uk; danny.werb@canterbury.ac.uk.*

## Appendix H: Survey answers

### Appendix H1: Professional1:

Table 5 Professional 1

|  |  |
| --- | --- |
| Question | Answer |
| In your opinion, what are the positive and negative aspects of the proposed report system? | The proposed report system likely has positive aspects such as promoting accountability, transparency, and providing a mechanism for addressing issues. However, it might also have negative aspects such as potential abuse, false reports, and increased workload for moderators or administrators. The effectiveness of the system will depend on its design, implementation, and how well it balances these factors. |
| The proposed report complies with the reporting requirements imposed by the organisation | Yes |
| How does the propose reporting system differ from your company reporting system? | Our company’s report is shorter, it does not include as many sections, the tools section is added by default in the report because it is included in the template. |
| Do you consider that the proposed report could be a standard in the sector? | Strongly Agree |
| In your opinion has it been difficult to create a report with the proposed report system? why? | The report is long, it took me a bit longer than I would have done, it was easy as it explains what to do in each section, thanks to this and the fact that there are 12 sections, it makes sure that there is content that should not be in certain sections. |
| Does the proposed report have more sections than your organisation’s report? | Yes |
| what aspects of the proposed report would you improve? | 1. Enhanced Introduction:  Add an introduction section before the executive summary. This can include the purpose of the report, the scope of the cybersecurity audit, and a brief summary of the methodology used. This prepares the reader for the technical details to follow.  2. Inclusion of a Business Impact Summary:  Add a section that discusses the potential business impact of the vulnerabilities. This may include the impact on confidentiality, integrity, and availability of systems, as well as any legal or reputational implications. This section can help contextualise the importance of the vulnerabilities in business terms.  3 Conclusion section:  Add a conclusion at the end of the report to recap the main findings, recommendations and suggested next step. This provides closure to the document and reinforces key points.  4. Visual Enhancements:  For the “OWASP Top 10 Summary” section, consider including both bar charts and pie charts to provide a richer visual comparison. Also, ensure that all graphs and tables are clear and well labelled for ease of understanding. |
| Do you think your supervisors would approve the implementation of the proposed report? | Strongly Agree |
| The proposed report complies with current standards (NIST, ISO27001). | No |
| Do you find the report long to read? | Strongly Agree |

### Appendix H2: Professional 2

Table 6 Professional 2

|  |  |
| --- | --- |
| Question | Answers |
| In your opinion, what are the positive and negative aspects of the proposed report system? | In my opinion there is nothing negative. The structure is clear and reflects all the sections of the assessment |
| The proposed report complies with the reporting requirements imposed by the organisation | Yes |
| How does the proposed reporting system differ from your company reporting system? | Only in the order of the sections, but the content is the same. |
| Do you consider that the proposed report could be a standard in the sector? | Strongly Agree |
| In your opinion has it been difficult to create a report with the proposed report system? why? | It has not been complicated, neither to make it nor to interpret it. |
| Does the proposed report have more sections than your organisation’s report? | No |
| what aspects of the proposed report would you improve? | Nothing |
| Do you think your supervisors would approve the implementation of the proposed report? | Strongly Agree |
| The proposed report complies with current standards (NIST, ISO27001). | Yes |
| Do you find the report long to read? | Disagree |

### Appendix H3: Professional 3

Table 7 Professional 3

|  |  |
| --- | --- |
| Question | Answers |
| In your opinion, what are the positive and negative aspects of the proposed report system? | Positives: Simplicity (all pieces of information are sorted by section and therefore easy to add and read), Thoroughness (wordlists, tools and exploits are all included, as well as a timeline, making it easy to reconstruct what a penetration tester did during an assignment),  Clarity (each section has clear instructions as to what goes into it and what does not) Negatives: Too much detail (many organizations will probably be uninterested in what tools and wordlists are used), No discussion of impact (what the money or reputation cost will be to a specific organization).. |
| The proposed report complies with the reporting requirements imposed by the organisation | Yes |
| How does the proposed reporting system differ from your company reporting system? | Our company pentest reports include a list of tested assets, as well as a section on systemic flaws in an organization’s security, and a section on (predicted) impact to the client. Similarly, our company does not detail specific tools or wordlists used. |
| Do you consider that the proposed report could be a standard in the sector? | Agree |
| In your opinion has it been difficult to create a report with the proposed report system? why? | Yes. Many client organizations have specific requirements for reporting, as well as different goals and priorities, which makes it difficult to find a standard that they all agree to. |
| Does the proposed report have more sections than your organisation’s report? | No |
| what aspects of the proposed report would you improve? | I would add a section for systemic issues (issues that are noticed many times during the pentest, such as outdated software, or lack of encryption on web traffic), as well as a section on impact to the client. |
| Do you think your supervisors would approve the implementation of the proposed report? | Agree |
| The proposed report complies with current standards (NIST, ISO27001). | Yes |
| Do you find the report long to read? | Disagree |

### Appendix H4: Professional 4

Table 8 Professional 4

|  |  |
| --- | --- |
| Question | Answers |
| In your opinion, what are the positive and negative aspects of the proposed report system? | Positive: It seems to be quite a detailed report, they want to give a lot of detail about the work done.  Negative: It depends on the nature of the report, whether it is an executive or technical report. But in either case I would remove sections 8, 11 and 12. In my opinion there is too much information. |
| The proposed report complies with the reporting requirements imposed by the organisation | I don’t know |
| How does the proposed reporting system differ from your company reporting system? | Points 8, 9 and 12 we do not expose them. The rest of the proposed report is quite similar. |
| Do you consider that the proposed report could be a standard in the sector? | Agree |
| In your opinion has it been difficult to create a report with the proposed report system? why? | It has not been difficult, it is very similar to the reports I make. |
| Does the proposed report have more sections than your organisation’s report? | Yes |
| what aspects of the proposed report would you improve? | I propose to make it shorter and more concise. |
| Do you think your supervisors would approve the implementation of the proposed report? | Agree |
| The proposed report complies with current standards (NIST, ISO27001). | I don’t know |
| Do you find the report long to read? | Strongly Agree |

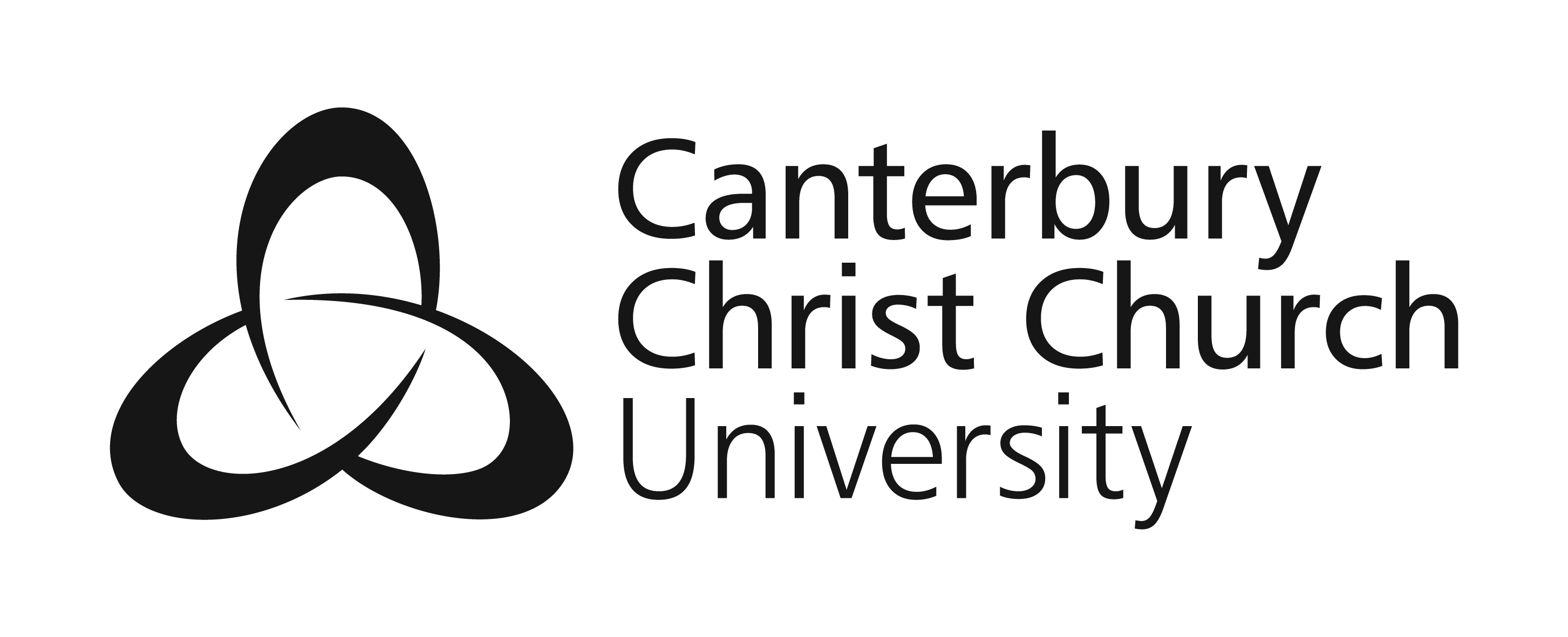
### Appendix H5: Professional 5

Table 9 Professional 5

|  |  |
| --- | --- |
| Question | Answers |
| In your opinion, what are the positive and negative aspects of the proposed report system? | It is a very clear and detailed reporting model, which can bring a lot of value to customers as they will have both an executive view understandable for non-technical employees and the detail of the exploitation of each vulnerability, evidence and mitigations for technical staff, development team, etc. This will be very useful for them to understand and remediate vulnerabilities found during the assessment. |
| The proposed report complies with the reporting requirements imposed by the organisation | Yes |
| How does the proposed reporting system differ from your company reporting system? | I can’t talk about my company’s For example, the timeline and tools used are usually included at the beginning and not after the executive summary, and there is usually no specific section for OWASP, but simply next to each vulnerability found, information regarding the OWASP category to which it belongs is added. |
| Do you consider that the proposed report could be a standard in the sector? | Agree |
| In your opinion has it been difficult to create a report with the proposed report system? why? | No, because normally in my company, the reports are usually as long as the proposed report |
| Does the proposed report have more sections than your organisation’s report? | Yes |
| what aspects of the proposed report would you improve? | The scope of the audit, the scope of scope of the audit, scope of testing |
| Do you think your supervisors would approve the implementation of the proposed report? | Agree |
| The proposed report complies with current standards (NIST, ISO27001). | I don’t know |
| Do you find the report long to read? | Disagree |

## Appendix I: Consent Form

### Appendix I1: Consent form 1:

****

**CONSENT FORM**

|  |  |
| --- | --- |
| **Title of Project:** | Evaluation of penetration testing reporting methods using CVSS4.0 |
| **Name of Researcher**: | Marco Carrasco |

**Contact details:**

|  |  |  |
| --- | --- | --- |
| **Address:** |  | N Holmes Rd, Canterbury CT1 1QU, United Kingdom |
|  |  |  |
|  |  |  |
|  |  |  |
| **Tel:** |  | +44 (0) 1227 921692 |
|  |  |  |
| **Email:** |  | mc1381@canterbury.ac.uk |

**Please initial box**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | I confirm that I have read and understand the participant information for the above project and have had the opportunity to ask questions. |  | X |
| 2. | (If applicable) I confirm that I agree to any audio and/or visual recordings. |  |  |
| 3. | I understand that any personal information that I provide to the researchers will be kept strictly confidential and in line with the University [Research Privacy Notice](https://www.canterbury.ac.uk/university-solicitors-office/data-protection/privacy-notices/privacy-notices.aspx) |  | X |
| 4. | I understand that my participation is voluntary and that I am free to withdraw my participation at any time, without giving a reason. |  | X |
| 5. | I agree to take part in the above project. |  | X |

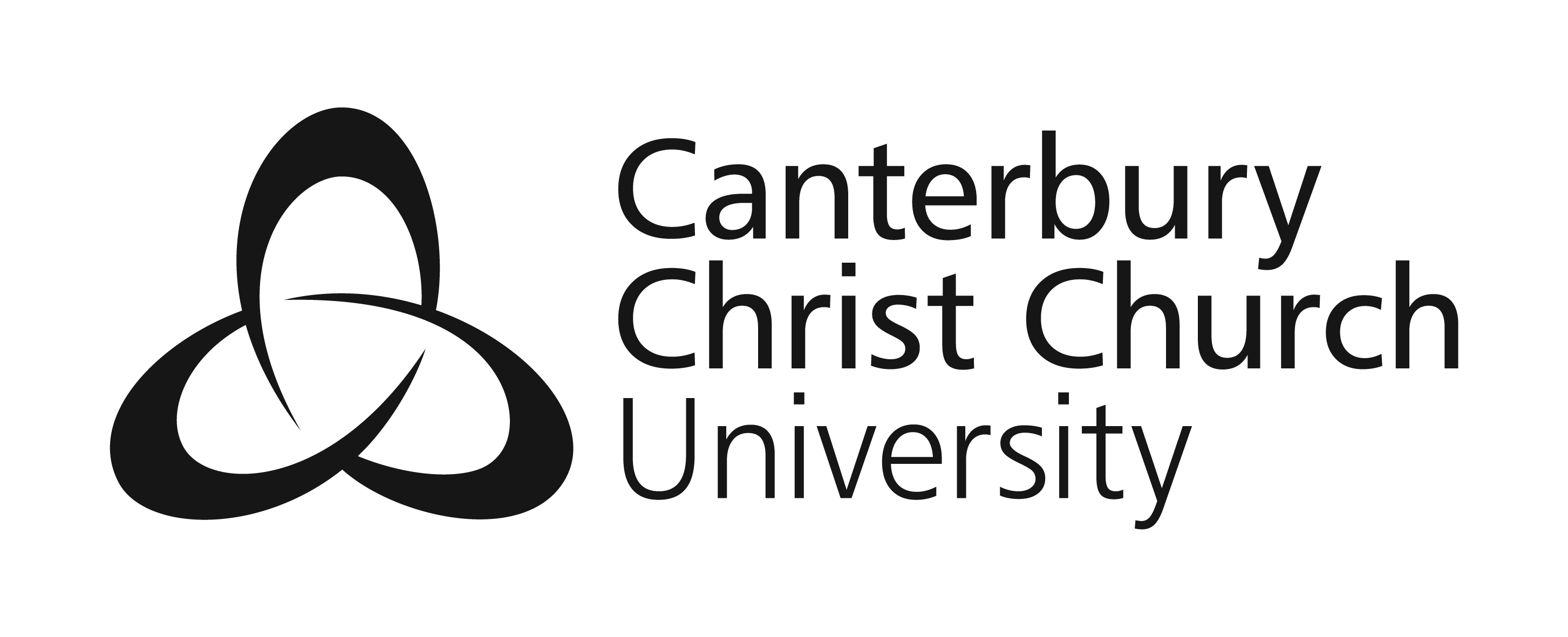
\_\_

|  |  |  |
| --- | --- | --- |
| Name of Participant: Pau Cañadillas | Date:29/03/2024 | Signature: Imagen que contiene Diagrama  Descripción generada automáticamente |
| Name of person taking consent *(if different from researcher)* | Date: | Signature: |
| Researcher: Marco | Date: 27/03/2024 | Signature: Un dibujo de una persona  Descripción generada automáticamente con confianza baja |

Copies: 1 for participant

1 for researcher

### Appendix I2: Consent form 2

****

**CONSENT FORM**

|  |  |
| --- | --- |
| **Title of Project:** | Evaluation of penetration testing reporting methods using CVSS4.0 |
| **Name of Researcher**: | Marco Carrasco |

**Contact details:**

|  |  |  |
| --- | --- | --- |
| **Address:** |  | N Holmes Rd, Canterbury CT1 1QU, United Kingdom |
|  |  |  |
|  |  |  |
|  |  |  |
| **Tel:** |  | +44 (0) 1227 921692 |
|  |  |  |
| **Email:** |  | mc1381@canterbury.ac.uk |

**Please initial box**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | I confirm that I have read and understand the participant information for the above project and have had the opportunity to ask questions. |  | X |
| 2. | (If applicable) I confirm that I agree to any audio and/or visual recordings. |  |  |
| 3. | I understand that any personal information that I provide to the researchers will be kept strictly confidential and in line with the University [Research Privacy Notice](https://www.canterbury.ac.uk/university-solicitors-office/data-protection/privacy-notices/privacy-notices.aspx) |  | X |
| 4. | I understand that my participation is voluntary and that I am free to withdraw my participation at any time, without giving a reason. |  | X |
| 5. | I agree to take part in the above project. |  | X |

\_\_

|  |  |  |
| --- | --- | --- |
| Name of Participant: Victoria Ibañez | Date:28/03/2024 | Signature: Diagrama  Descripción generada automáticamente |
| Name of person taking consent *(if different from researcher)* | Date: | Signature: |
| Researcher: Marco | Date: 27/03/2024 | Signature: Un dibujo de una persona  Descripción generada automáticamente con confianza baja |

Copies: 1 for participant

1 for researcher

### Appendix I3: Consent form 3

****

**CONSENT FORM**

|  |  |
| --- | --- |
| **Title of Project:** | Evaluation of penetration testing reporting methods using CVSS4.0 |
| **Name of Researcher**: | Marco Carrasco |

**Contact details:**

|  |  |  |
| --- | --- | --- |
| **Address:** |  | N Holmes Rd, Canterbury CT1 1QU, United Kingdom |
|  |  |  |
|  |  |  |
|  |  |  |
| **Tel:** |  | +44 (0) 1227 921692 |
|  |  |  |
| **Email:** |  | mc1381@canterbury.ac.uk |

**Please initial box**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | I confirm that I have read and understand the participant information for the above project and have had the opportunity to ask questions. |  | X |
| 2. | (If applicable) I confirm that I agree to any audio and/or visual recordings. |  |  |
| 3. | I understand that any personal information that I provide to the researchers will be kept strictly confidential and in line with the University [Research Privacy Notice](https://www.canterbury.ac.uk/university-solicitors-office/data-protection/privacy-notices/privacy-notices.aspx) |  | X |
| 4. | I understand that my participation is voluntary and that I am free to withdraw my participation at any time, without giving a reason. |  | X |
| 5. | I agree to take part in the above project. |  | X |

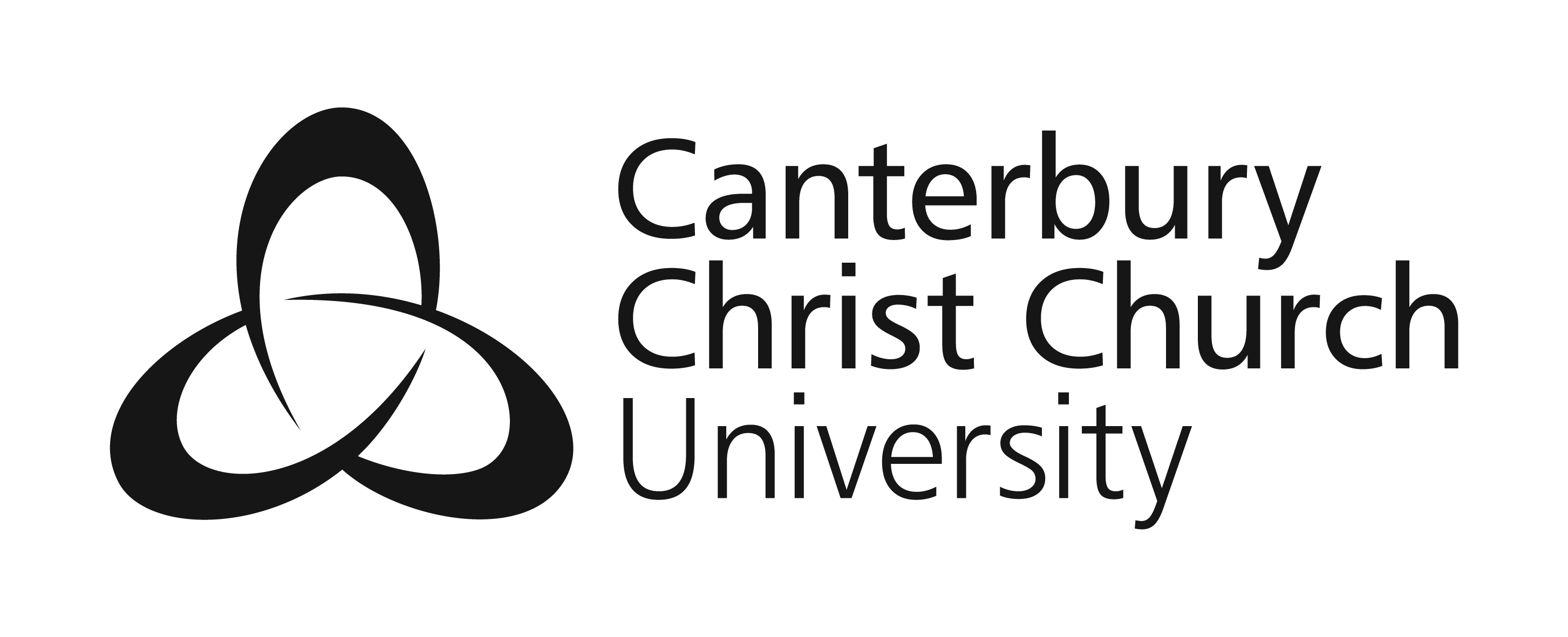
\_\_

|  |  |  |
| --- | --- | --- |
| Name of Participant:  Thomas E.Mason | Date: 29/03/2024 | Signature: |
| Name of person taking consent *(if different from researcher)* | Date: | Signature: |
| Researcher: Marco | Date: 27/03/2024 | Signature: Un dibujo de una persona  Descripción generada automáticamente con confianza baja |

Copies: 1 for participant

1 for researcher

### Appendix I4: Consent form 4

****

**CONSENT FORM**

|  |  |
| --- | --- |
| **Title of Project:** | Evaluation of penetration testing reporting methods using CVSS4.0 |
| **Name of Researcher**: | Marco Carrasco |

**Contact details:**

|  |  |  |
| --- | --- | --- |
| **Address:** |  | N Holmes Rd, Canterbury CT1 1QU, United Kingdom |
|  |  |  |
|  |  |  |
|  |  |  |
| **Tel:** |  | +44 (0) 1227 921692 |
|  |  |  |
| **Email:** |  | mc1381@canterbury.ac.uk |

**Please initial box**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | I confirm that I have read and understand the participant information for the above project and have had the opportunity to ask questions. |  | X |
| 2. | (If applicable) I confirm that I agree to any audio and/or visual recordings. |  |  |
| 3. | I understand that any personal information that I provide to the researchers will be kept strictly confidential and in line with the University [Research Privacy Notice](https://www.canterbury.ac.uk/university-solicitors-office/data-protection/privacy-notices/privacy-notices.aspx) |  | X |
| 4. | I understand that my participation is voluntary and that I am free to withdraw my participation at any time, without giving a reason. |  | X |
| 5. | I agree to take part in the above project. |  | X |

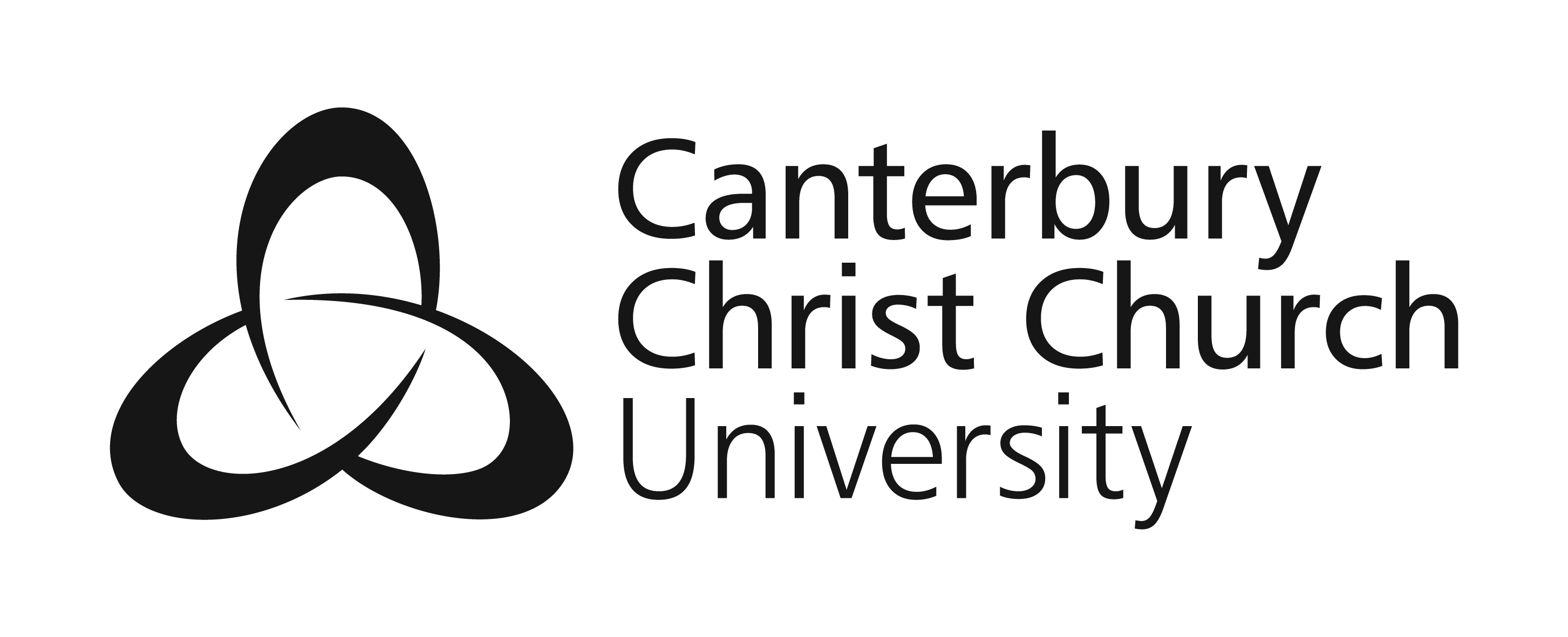
\_\_

|  |  |  |
| --- | --- | --- |
| Name of Participant: Alex Hernandez | Date: 29/03/2024 | Signature: Imagen que contiene Diagrama  Descripción generada automáticamente |
| Name of person taking consent *(if different from researcher)* | Date: | Signature: |
| Researcher: Marco | Date: 27/03/2024 | Signature: Un dibujo de una persona  Descripción generada automáticamente con confianza baja |

Copies: 1 for participant

1 for researcher

### Appendix I5: Consent Form 5

****

**CONSENT FORM**

|  |  |
| --- | --- |
| **Title of Project:** | Evaluation of penetration testing reporting methods using CVSS4.0 |
| **Name of Researcher**: | Marco Carrasco |

**Contact details:**

|  |  |  |
| --- | --- | --- |
| **Address:** |  | N Holmes Rd, Canterbury CT1 1QU, United Kingdom |
|  |  |  |
|  |  |  |
|  |  |  |
| **Tel:** |  | +44 (0) 1227 921692 |
|  |  |  |
| **Email:** |  | mc1381@canterbury.ac.uk |

**Please initial box**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | I confirm that I have read and understand the participant information for the above project and have had the opportunity to ask questions. |  | X |
| 2. | (If applicable) I confirm that I agree to any audio and/or visual recordings. |  |  |
| 3. | I understand that any personal information that I provide to the researchers will be kept strictly confidential and in line with the University [Research Privacy Notice](https://www.canterbury.ac.uk/university-solicitors-office/data-protection/privacy-notices/privacy-notices.aspx) |  | X |
| 4. | I understand that my participation is voluntary and that I am free to withdraw my participation at any time, without giving a reason. |  | X |
| 5. | I agree to take part in the above project. |  | X |

\_\_

|  |  |  |
| --- | --- | --- |
| Name of Participant: Marcos Espínola | Date: 04/04/2024 | Signature: Marcos Espínola |
| Name of person taking consent *(if different from researcher)* | Date: | Signature: |
| Researcher: Marco | Date: 27/03/2024 | Signature: |

Copies: 1 for participant

1 for researcher

## Appendix J: Research Questions

1ºIn your opinion, what are the positive and negative aspects of the proposed report system?

1º to know from a professional point of view the improvements or disadvantages of the system. This is useful for the research to obtain a 2nd opinion on which sections are well implemented, and which aspects can be improved in the organisations of the interviewees.

2º The proposed report complies with the reporting requirements imposed by the organisation.

2º Whether the proposed report complies with the requirements and the mandatory content imposed in your company.

3º How does the propose reporting system differ from your company reporting system?

3º Whether the system is very different from the one used by the different organisations, as there is no general standard model. This is useful for research to see whether the template is easy to adapt.

4º Do you consider that the proposed report could be a standard in the sector?

4º How likely it is that the report can become a standard for the sector, and replace the report that companies do in-house.

5º In your opinion has it been difficult to create a report with the proposed report system? why?

5º whether the auditor has made too much or too little difference or whether the format is too long to write (whether it took longer, whether the information described at each stage of the new system is in external sources, or whether it took longer to find it). This is useful for research to see if the new model is more costly (in time) and to see how the organisations’ information systems model varies.

6º Does the proposed report have more sections than your organisation’s report?

6º Since each client has specific needs, it is advisable to adapt to the needs, the objective of this question is to see if in the interviewee’s company the report is too long or has more sections than the one they usually write.

7º what aspects of the proposed report would you improve?

7º From a professional point of view, what aspects of the report could be improved to adapt it to the context of the organisation. This helps the research to see possible improvements and new sections.

8º Do you think your supervisors would approve the implementation of the proposed report?

8º whether you think your supervisors/analyst team in your company would approve of the standardisation of the proposed report in your company, certain organisations have specific requirements, in addition to standards such as NIST.

9º The proposed report complies with current standards (NIST, ISO27001).

9º whether the proposed report complies with the requirements of current standards such as NIST or ISO27001, this is useful to know if the report needs to be corrected to comply with the standard.

10º Do you find the report long to read?

10th if the professional thinks the report has too many sections, or is too long to read/understand, this helps the overall understanding of the document and affects the audiences.

## Appendix K: Evaluation

What would a report using the new CVSS4.0 (instead of the classic CVSS 3.1) look like?

This question has not been answered, the 2 versions have been compared in literature review but it has been shown what the result of the CVSS4.0 calculation would look like in a report.

How could the process of reporting be standardized?

This question has been answered, through the creation of a report and a survey. survey has been used to find out if it can be standardised and how it differs from other companies' reports of other companies

Is it effective to create a framework for reporting?

This question has not been answered, no analysis of the impact of reporting on companies has been carried out.

Are the automatic reporting tools easy to understand?

Part of the question has been answered, an automatic reporting tool has been analysed, and the effort involved has been analysed analysed the effort involved in using it to make a report but did not analyse whether they are easy to use at a more complex level.

“The creation of an effective and efficient reporting method may enhance cyber decision-making in companies. This improvement could lead to better prevention of cyber-attacks and cost savings through securing infrastructure. The aim is to create an effective reporting method to improve decision-making, enhance cybersecurity, and reduce infrastructure security costs.”

The hypothesis cannot be confirmed or rejected, no relationship between decision-making and the structure of the report has been studied, but it has been found that a cybersecurity report has to have a high standard of clarity and detail to be understandable for both technical and non-technical audiences, and also thanks to the research on the reporting infrastructure (manual vs. automatic), it has been found that manual reporting is adequate, making part of the hypothesis true and saving costs by securing infrastructure.