**Report Template**

**Assessment cover**

**STUDENTS, PLEASE COPY THIS PAGE AND USE AS THE COVER PAGE FOR YOUR SUBMISSION**

|  |  |  |  |
| --- | --- | --- | --- |
| Module No: | **COMP4035** | Module title: | **Computer Science Application** |

|  |  |
| --- | --- |
| Assessment title : | **Cybersecurity Coursework- Security Assessment and Recommendations** |

|  |  |
| --- | --- |
| Due date and time**:** | **02/05/2025 10:00** |

|  |  |
| --- | --- |
| Estimated total time to be spent on assignment: | 30 hours per student |

**LEARNING OUTCOMES**

|  |
| --- |
| **On successful completion of this module, students will be able to achieve the module following learning outcomes (LOs):** *LO numbers and text copied and pasted from the module descriptor* |
| LO 3: Understand the principles of cyber security, secure design and apply the principles of penetration testing |

|  |  |
| --- | --- |
| **Engineering Council AHEP4 LOs assessed (from S1 2022-23)**  *LOs copied and pasted from the AHEP4 matrix* | |
|  |  |
|  |  |
|  |  |
|  |  |

**STUDENT NAMES (ONLY IF GROUP ASSIGNMENT, OTHERWISE ANONYMOUS)**

|  |  |  |
| --- | --- | --- |
| **Student No:** | **Student Name:** | **Group Name and Number:** |
| **1.19334208** | **Salih Mirza Doğan** | **SET 4: GROUP 33** |
| **2.19337507** | **Nick Jones** | **SET 4: GROUP 33** |
| **3.19334254** | **Tom Woods** | **SET 4: GROUP 33** |
|  |  |  |

**Statement of Compliance *(please tick to sign)***

I declare that the work submitted is my own and that the work I submit is fully in accordance with the University regulations regarding assessments *(*[*www.brookes.ac.uk/uniregulations/current*](http://www.brookes.ac.uk/uniregulations/current)*)*

Part 1: Introduction:

The system for this security assessment is Monzo, a fully digital bank that operates without any physical branches. This model is rooted in a cloud-first infrastructure, supported by mobile and web applications that provide streamlined, always-available financial services.

Unlike legacy banks, Monzo eliminates the overhead of maintaining physical locations, reducing operational costs and improving user convenience through digital-only service delivery (Disrupto, 2024).

This digital architecture, while efficient and customer-centric, brings inherent security challenges. Monzo’s platform processes large volumes of sensitive customer data—including personal identity information and financial transactions–which are highly attractive targets for malicious actors. Consequently, the integrity, confidentiality, and availability of this data are paramount.

Monzo has adopted a microservices architecture that runs entirely in a secure, containerized cloud environment. Each service is isolated and governed by strict communication policies,

Ensuring minimal exposure and reduced blast radius in the event of a breach. The system operates on a zero-trust model–workloads are not inherently trusted, and every request must be authenticated and authorized explicitly (Monzo 2022). These principles enable rapid scalability while maintaining tight security controls.

Security is embedded into the development lifecycle through proactive collaboration between engineers and security teams. Threat modeling exercises are routinely conducted to anticipate and mitigate potential attack vectors before they can be exploited. Moreover, any additions to the infrastructure are rigorously reviewed to ensure alignment with Monzo’s overarching security posture (Monzo, 2022)

By combining the agility of digital banking with embedded, system-level security practices Monzo exemplifies how financial technology providers must adapt in a climate of rising cyber risk. This assessment will critically evaluate Monzo’s current security design, identify areas of vulnerability, and recommend actionable improvements to enhance the resilience of the platform.

Disrupto. (2024, September 12). *The benefits of online banking for banks*. Disrupto. Retrieved April 4, 2025, from<https://www.disrupto.co.uk/blogs/the-benefits-of-online-banking-for-banks/>

Monzo. (2022, March 31). *How we secure Monzo’s banking platform*. Monzo Bank.<https://monzo.com/blog/2022/03/31/how-we-secure-monzos-banking-platform>

Section 2: Methodology:

For Monzo, ı felt that security architecture review would be the most important methodology as it focuses on the core structure of the system and how security is built into these systems. A security architecture review identifies any potential weak points by analyzing how data flows throughout the system. Given how Monzo uses a lot of microservices (most notably Amazon’s AWS and others), a security architecture review ensures that how Monzo interacts with these microservices is secure. us

The process of a security architecture review starts with defining the scope of the review. This includes identifying specific areas/systems you want to assess. In Monzo’s case, this could be assessing the backend services or cloud infrastructure such as AWS. Making clear objectives for the review in this section is important as it allows you to evaluate whether your review was successful and/or effective.

The next step is gathering information by looking at any documentation related to the system. This could be data flow diagrams, sections of cod,e, or configuration files. Once relevant documentation has been gathered, you will then need to verify that the information in the documents is correct by talking to the relevant teams.

After the information has been checked, you can start the analysis. An effective way of doing this is by leveraging different methods and tools such as checking guidelines, and frameworks and even using automated tools and covering “CIA” – confidentiality, integrity, and availability. Whilst checking the system is a key aspect of a security architecture review, you also want to ensure that incident response is checked so that if an attacker managed to get in, you could minimize the losses.

Penultimately, you would report your findings. This should be done in a clear and concise manner where you illustrate strengths and weaknesses, showing any gaps/issues, and giving recommendations to improve the security of the system. Once the report has been documented, you can discuss it with relevant teams within Monzo such as the developers, and tailoring the information to whichever team you are talking to. Not only this but getting feedback from them is important as it can allow you to perform a better review in the future.

Finally, you monitor the progress to find out how effective the review was, ensuring that the security issues were addressed and that the overall security of the system is improved over time. This could mean that you use automated tools to check this or running tests.

*How can stakeholders ensure security architecture reviews are effective? (no date)*

*references:*

*How can stakeholders ensure security architecture reviews are effective?* (no date) [*www.linkedin.com*](http://www.linkedin.com/). Available at: <https://www.linkedin.com/advice/3/how-can-stakeholders-ensure-security-architecture-62y1c> (Accessed: 11 April 2025).

*Monzo Case Study* (2025) *Google Cloud*. Available at: <https://cloud.google.com/customers/monzo-bank> (Accessed: 18 April 2025).

Section 3: Pentesting

Using Penetration Testing to Assess the Security of Monzo’s Online Banking Platform:

Penetration testing (often called pen testing) is a way to simulate attacks on a system to find vulnerabilities before real attackers can exploit them. This process is very important for a fully digital bank like Monzo because it handles sensitive customer information and financial transactions. Monzo's reliance on mobile apps and cloud services makes system security crucial for user protection and trust.

Monzo's infrastructure relies on AWS, utilizing features like AWS WAF and Nitro Enclaves. They employ tokenization to avoid handling credit card details. However, attackers may still target mobile app binaries, API endpoints, or third-party services.

Types of Penetration Testing:

1) Black Box Testing: The tester has no inside knowledge and attempts to identify vulnerabilities by interacting with the system as an external attacker.

2) White Box Testing: The tester knows everything about the system, including code and architecture. This helps them focus on specific areas like session handling or encryption methods.

3) Grey Box Testing: which simulates insider threats or limited-access users to test internal security controls

Common attack scenarios include phishing simulations, brute-force login attempts, man-in-the-middle (MitM) attacks to test encryption, and malware emulation to assess app behavior on compromised devices. Additionally, third-party API assessments help evaluate the security of external services.

The typical pen testing process involves five phases: reconnaissance (e.g., Shodan),

Scanning (Nmap, Nessus), gaining access (Metasploit, Burp Suite), maintaining access, and covering tracks to test detection systems.

In conclusion, pen-testing offers Monzo a realistic, hands-on evaluation of its security posture and ensures continuous improvement beyond what automated tools or audits can provide.

Section 4: Recommendations and Personal Reflection

Based on the security assessment and penetration testing of Monzo’s online banking platform, I believe there are a few ways to make their security even better and more secure.

Firstly, Monzo should continue regular penetration testing, especially focusing on mobile apps and third-party APIs, which are often easy targets for attackers. Social engineering tests like phishing simulations would also help strengthen employee awareness and reduce human errors.

Secondly, setting up a bug bounty program could be a good idea. This would allow ethical hackers to report vulnerabilities, giving Monzo extra protection by having more eyes checking for hidden issues.

Also, even though Monzo follows a strong zero-trust model, it should make sure that all third-party services meet the same security standards. Regular audits of these services could help prevent supply chain attacks.

From my perspective, working on this project made me realize how important it is to think beyond just technical problems. Even a company like MONZO NEEDS to keep improving all the time. THİS assessment also showed me how penetration testing is not just about using tools but also about understanding real-world attack methods. Overall I can say that it helped me see how important it is to combine technical knowledge with creative thinking in cybersecurity.

5. TeamWork:

Our group consisted of Tom Woods(methodology), Nick Jones(He did the introduction), and me. To collaborate and divide the work fairly, we held four online meetings during this project. All meetings were held via Google Meet, and the minutes were uploaded to the shared Google Drive folder as required.

 All meeting minutes have been uploaded to our shared Google Drive folder as required. The folder has been shared with modules staff and includes meeting notes for Weeks 7 through 10

 6. References:

**Monzo (2022).** How we secure Monzo’s banking platform

–[https://monzo.com/blog/2022/03/31/how-we-secure-monzos-banking-platform[](https://monzo.com/blog/2022/03/31/how-we-secure-monzos-banking-platform%5baccesseed)[Accessed: 3 May 2025]

Almomani, M. (2021) *The effectiveness of penetration testing methodologies in improving an organization's cyber security: A case study of SMEs in the UK*. MSc Dissertation. University of Liverpool. Available at:<https://livrepository.liverpool.ac.uk/3138094/1/200928649_Sep2021.pdf> (Accessed: 20 April May 2025).

BlueVoyant (n.d.) *Penetration Testing: A Complete Guide to Process, Types, and Tools.* Available at:<https://www.bluevoyant.com/knowledge-center/penetration-testing-complete-guide-to-process-types-and-tools> (Accessed: 1 May 2025).

BrightSec (n.d) *Penetration testing types: 7 types of pen tests & how to use them*. Available at:<https://www.brightsec.com/blog/penetration-testing-types/> (Accessed: 24 April 2025).

Cetera (n.d). *What is penetration testing? Stages, techniques, types & benefits*. Available at:<https://certera.com/blog/what-is-penetration-testing-stages-techniques-types-benefits/> (Accessed: 26 April 2025).

OWASP (n.d) *OWASP Top Ten*. Available at:<https://owasp.org/www-project-top-ten/> (Accessed: 25 April 2025).

Section 7:

**Google Drive Folder Link:**  
1)<https://drive.google.com/drive/u/0/folders/1g3nJywKuCLHy-H9Vy3IAZUwYT7TOwv8J>

2)<https://drive.google.com/drive/folders/1g3nJywKuCLHy-H9Vy3IAZUwYT7TOwv8J?usp=drive_link>