APPLICATION FOR ETHICAL APPROVAL

In order for research to result in benefit and minimise risk of harm, it must be conducted ethically.

The University follows the OECD Frascati manual definition of **research activity**: "creative work undertaken on a systematic basis in order to increase the stock of knowledge, including knowledge of man, culture and society, and the use of this stock of knowledge to devise new applications". As such this covers activities undertaken by members of staff, postgraduate research students, and both taught postgraduate and undergraduate students working on dissertations/projects.

The individual undertaking the research activity is known as the "principal researcher".

This form must be completed and approved prior to undertaking any research activity.

SECTION A: About You (Principal Researcher)

1	Full Name:	Jay Shaileshbhai Lad
2	Student Number:	2504388
3	Email address:	2504388@student.uwtsd.ac.uk
4	Programme of Study:	MSc Cybersecurity and Digital Forensics
5	Supervisor:	Fahad Ahmed

SECTION B: Internal and External Ethical Guidance Materials

	Please list the core ethical guidance documents that have been referred to during the completion of this form (including any discipline-specific codes of research ethics, location-specific dodes of research ethics, and also any specific ethical guidance relating to the proposed methodology). Please tick to confirm that your research proposal adheres to these codes and guidelines. You may add rows to this table if needed.	
1	**UWTSD Research Ethics & Integrity Code of Practice**	☒
2	**UWTSD Research Data Management Policy**	☒
3		☐
4		☐

SECTION C: Details of Research Activity

1	Indicative title:	VULNERABILITY ASSESSMENT AND PENETRATION TESTING TO ENHANCE WEB APPLICATION SECURITY		
2	Proposed start date:	June 2026	Proposed end date:	September 2026
	Introduction to the Research (maximum 300 words in each section) **Ensure that you write for a <u>Non-Specialist Audience</u> when outlining your response to the three points below:** • *Purpose of Research Activity*			

	• *Proposed Research Question* • *Aims of Research Activity* • *Objectives of Research Activity* Demonstrate, briefly, how **Existing Research** has informed the proposed activity and explain • *What the research activity will add to the body of knowledge* • *How it addresses an area of importance.*
3	**Purpose of Research Activity** The purpose of this research is to conduct a Vulnerability Assessment and Penetration Testing (VAPT) exercise on a self-developed, locally hosted Loyalty Card Management System, in order to identify security vulnerabilities, remediate them at source-code level, and verify the effectiveness of the remediation through re-testing. The research follows the OWASP Top Ten framework to assess common web application vulnerabilities (including SQL Injection, Cross-Site Scripting, and Cross-Site Request Forgery), and extends beyond this to identify and mitigate business-logic vulnerabilities specific to loyalty-reward platforms (price tampering, order-cancellation IDOR, and points double-spending). The aim is to produce a fully remediated and re-verified system, and to contribute a reusable methodology for assessing the security of loyalty-based e-commerce applications.
4	**Research Question** What technical and business-logic vulnerabilities are present in a Loyalty Card Management System when assessed against the OWASP Top Ten framework and domain-specific business-logic analysis, and to what extent can these vulnerabilities be effectively remediated and verified through source-code-level fixes and re-testing? Sub-questions: 1. What technical vulnerabilities, assessed against the OWASP Top Ten, are present in the baseline implementation of the system? 2. To what extent can source-code-level remediation resolve the identified technical vulnerabilities, and how can this be verified? 3. What business-logic vulnerabilities exist in the loyalty-points and order-management workflows that a generic OWASP-based assessment would not detect? 4. How effectively can these business-logic vulnerabilities be mitigated through server-side enforcement and atomic database operations?
5	**Aims of Research Activity** The aim of this project is to assess, remediate and re-verify the security of a locally hosted Loyalty Card Management System through an applied VAPT methodology that combines OWASP-aligned technical testing with domain-specific business-logic analysis. The specific aims are to: 1. Design and implement a functionally representative Loyalty Card Management System (customer registration, authentication, dashboard, shop, orders, rewards redemption, and an administrative panel). 2. Conduct a baseline VAPT assessment against the OWASP Top Ten using automated tools (OWASP ZAP, Nikto, SQLMap) supported by manual verification with Burp Suite Community Edition. 3. Remediate every confirmed vulnerability at source-code level and document the precise changes applied. 4. Identify and mitigate business-logic vulnerabilities specific to a loyalty-reward platform, namely price tampering, order-cancellation IDOR, and points double-spending. 5. Establish a re-testing methodology to verify that remediated controls function as intended. 6. Evaluate the overall security improvement achieved and produce actionable recommendations for future development.
6	**Objectives of Research Activity** 1. To develop a functionally complete Loyalty Card Management System (PHP/MySQL) incorporating customer registration, authentication, a points dashboard, a shop and order workflow, rewards redemption, and an administrative panel, hosted in an isolated local test environment. 2. To perform a baseline security assessment of the system using automated scanning tools (OWASP ZAP, Nikto, SQLMap) and manual penetration testing (Burp Suite Community Edition), guided by the OWASP Top Ten framework. 3. To manually verify every automated scanning result before classifying it as a confirmed vulnerability, ensuring findings are evidence-based rather than tool-generated assumptions.

	4. To implement source-code-level remediation for every confirmed technical vulnerability, including Cross-Site Request Forgery protection, security headers, session-cookie hardening, brute-force lockout, password-reset security, email verification, password complexity policy, and bot protection. 5. To identify, demonstrate, and mitigate three business-logic vulnerabilities specific to the loyalty-points economy: price tampering in order placement, Insecure Direct Object Reference (IDOR) in order cancellation, and race-condition double-spending in points redemption. 6. To re-test the remediated system against the original baseline findings, providing before/after evidence of the security improvement achieved. 7. To critically evaluate the results against the research questions and produce recommendations for future security practice in comparable systems.
	Proposed data collection methods (maximum 600 words) Provide a brief summary of all the methods that **may** be used in the research activity to collect data, making it clear what specific techniques may be used. If methods other than those listed in this section are deemed appropriate later, additional ethical approval for those methods will be needed. You do not need to justify the methods here, but should instead describe how you intend to collect the data necessary for you to complete your project.
7	This research involves no human participants, personal data, or third-party systems. All data is technical, generated entirely from a Loyalty Card Management System that I designed and built myself, hosted in an isolated local environment (XAMPP server, tested from a separate Kali Linux VM under my own control). Data collection methods: 1. **Automated scanning** — OWASP ZAP, Nikto, and SQLMap generate scan logs and vulnerability alerts. 2. **Manual penetration testing** — Burp Suite is used to intercept, modify, and replay HTTP requests to verify vulnerabilities (CSRF, price tampering, IDOR, double-spending). 3. **Screenshots** — Captured at each testing stage as evidence. 4. **Database inspection** — phpMyAdmin used to verify test outcomes (e.g. points balance changes). 5. **Application logs** — Audit logs and login-attempt records reviewed to confirm security-control behaviour. 6. **Browser developer tools** — Used to inspect headers, cookies, and session behaviour.

SECTION D: Scope of Research Activity

	Will the research activity include:	**YES**	**NO**
1	Use of a questionnaire or similar research instrument?	☐	☒
2	Use of interviews?	☐	☒
3	Use of focus groups?	☐	☒
4	Use of participant diaries?	☐	☒
5	Use of video or audio recording?	☐	☒
6	Use of computer-generated log files?	☒	☐
7	Participant observation with their knowledge?	☐	☒
8	Participant observation without their knowledge?	☐	☒
9	Access to personal or confidential information without the participants' specific consent?	☐	☒
10	Administration of any questions, test stimuli, presentation that may be experienced as physically, mentally or emotionally harmful / offensive?	☐	☒
11	Performance of any acts which may cause embarrassment or affect self-esteem?	☐	☒
12	Investigation of participants involved in illegal activities?	☐	☒

13	Use of procedures that involve deception?	☐	☒
14	Administration of any substance, agent or placebo?	☐	☒
15	Working with live vertebrate animals?	☐	☒
16	Procedures that may have a negative impact on the environment?	☐	☒
17	Other primary data collection methods. Please indicate the type of data collection method(s) below.	☐	☒
	Details of any other primary data collection method:		

If you have ticked NO to every question then the research activity is (ethically) low risk and you may skip section E and continue to section F.

If YES to any question, then no research activity should be undertaken until full ethical approval has been obtained.

SECTION E: Intended Participants

	Who are the intended participants:	**YES**	**NO**
1	Students or staff at the University?	☐	☒
2	Adults (over the age of 18 and competent to give consent)?	☐	☒
3	Vulnerable adults?	☐	☒
4	Children and Young People under the age of 18? (Consent from Parent, Carer or Guardian will be required)	☐	☒
5	Prisoners?	☐	☒
6	Young offenders?	☐	☒
7	Those who could be considered to have a particularly dependent relationship with the investigator or a gatekeeper?	☐	☐
8	People engaged in illegal activities?	☐	☒
9	Others. Please indicate the participants below, and specifically any group who may be unable to give consent.	☐	☒
	Details of any other participant groups:		

	Participant numbers and source Provide an estimate of the expected number of participants. How will you identify participants and how will they be recruited?	
10	How many participants are expected?	N/A
11	Who will the participants be?	N/A
12	How will you identify the participants?	N/A

	Information for participants:	**YES**	**NO**	**N/A**

13	Will you describe the main research procedures to participants in advance, so that they are informed about what to expect?	☐	☐	☒
14	Will you tell participants that their participation is voluntary?	☐	☐	☒
15	Will you obtain written consent for participation?	☐	☐	☒
16	Will you explain to participants that refusal to participate in the research will not affect their treatment or education (if relevant)?	☐	☐	☒
17	If the research is observational, will you ask participants for their consent to being observed?	☐	☐	☒
18	Will you tell participants that they may withdraw from the research at any time and for any reason?	☐	☐	☒
19	With questionnaires, will you give participants the option of omitting questions they do not want to answer?	☐	☐	☒
20	Will you tell participants that their data will be treated with full confidentiality and that, if published, it will not be identifiable as theirs?	☐	☐	☒
21	Will you debrief participants at the end of their participation, in a way appropriate to the type of research undertaken?	☐	☐	☒
22	If NO to any of above questions, please give an explanation			
	You should be able to tick YES for all of these questions. If not, then explain why not in this box. N/A			

	Information for participants:	**YES**	**NO**	**N/A**
24	Will participants be paid?	☐	☐	☒
25	Is specialist electrical or other equipment to be used with participants?	☐	☐	☒
26	Are there any financial or other interests to the investigator or University arising from this study?	☐	☐	☒
27	Will the research activity involve deliberately misleading participants in any way, or the partial or full concealment of the specific study aims?	☐	☐	☒
28	If YES to any question, please provide full details			
	You should be able to tick NO for most of these questions. For any cases that you have ticked YES then provide details in this box. If you are using cameras/voice recorders to record interviews then please state that in this box. N/A			

SECTION F: Anticipated Risks

	Outline any anticipated risks that may adversely affect any of the participants, the researchers and/or the University, and the steps that will be taken to address them.	
1	**Risks to participants** For example: sector-specific health & safety, emotional distress, financial disclosure, physical harm, transfer of personal data, sensitive organisational information. If you have identified in section D that there are no participants then enter N/A and go skip to question 3.	
	Risk to participants: There are always risks. Do not write N/A unless you have no participants. N/A There are no human participants in this research. The study involves only technical security testing (Vulnerability Assessment and Penetration Testing) conducted against a self-developed application hosted entirely within an isolated local test environment under my own	*How you will mitigate the risk to participants:* *(this box should expand as you type)*

	control. No third parties, live systems, or real user data are involved at any stage, and no personal, financial, health-related, or organisationally sensitive information is collected, processed, or disclosed as part of this research.	
2	If research activity may include sensitive, embarrassing or upsetting topics (e.g. sexual activity, drug use) or issues likely to disclose information requiring further action (e.g. criminal activity), give details of the procedures to deal with these issues, including any support/advice (e.g. helpline numbers) to be offered to participants. Note that where applicable, consent procedures should make it clear that if something potentially or actually illegal is discovered in the course of a project, it may need to be disclosed to the proper authorities	
	N/A This research does not involve human participants and does not cover sensitive, embarrassing, or upsetting topics such as sexual activity, drug use, or criminal activity. The project is a purely technical Vulnerability Assessment and Penetration Testing exercise conducted against a self-developed application within an isolated local test environment. No third-party systems, live production environments, or real user data are targeted at any stage, and no scenario requiring disclosure to external authorities is anticipated to arise from this work.	
3	**Risks to the investigator** For example: personal health & safety, physical harm, emotional distress, risk of accusation of harm/impropriety, conflict of interest	
	Risk to the investigator: There are always risks. Do not write NA. 1. Risk of accusation of unauthorised access, hacking, or impropriety, since penetration testing techniques (vulnerability scanning, request interception, payload injection, exploitation attempts) closely resemble the actions of a malicious attacker if discovered or misunderstood by a third party. 2. Risk of accidental disruption or corruption of the test environment (e.g. database corruption during business-logic testing such as concurrent-request/race-condition testing on the points-redemption system). 3. Risk of accidentally targeting an unintended or unauthorised system if a testing tool is misconfigured (e.g. an incorrect target IP/URL entered into a scanning tool). 4. General eye strain, fatigue, and prolonged sedentary posture associated with extended periods of screen-based testing and documentation work. **How you will mitigate the risk to the investigator:** 1. All testing is conducted exclusively against a system that I personally designed, built, and own, hosted entirely within an isolated local environment (a XAMPP server on my own machine) with no connection to any live, production, or third-party network. Testing tools are run	*How you will mitigate the risk to the investigator:* *(this box should expand as you type)*

	from a separate, self-controlled Kali Linux virtual machine. A clear, documented scope (Section 1.6 of the dissertation) confines all activity to this self-owned system, and no external, third-party, or publicly accessible website is targeted at any stage. 2. Only fictitious test/dummy data is used throughout, regular local backups of the test database are taken before conducting higher-risk tests (e.g. race-condition testing), and the entire environment is contained within a virtual machine that can be reverted to a clean snapshot if disrupted. 3. Before running any scanning or exploitation tool, the target URL/IP is manually verified against the known local address of my own test environment (e.g. confirming the VirtualBox NAT address or localhost) before initiating any scan or attack. 4. Regular breaks are scheduled during extended testing sessions, and an ergonomic workstation setup is used to reduce physical strain.	
4	**University/institutional risks** For example: adverse publicity, financial loss, data protection	
	Risk to the University: There are always risks. Do not write NA. 1. Risk of adverse publicity or reputational harm if the project, or testing techniques described within it, were to be misinterpreted as an actual attack against a live system, or if the dissertation's documented vulnerabilities and exploitation techniques were misused by a third party if published or shared without appropriate care. 2. Risk of data protection concerns if any real personal or institutional data were inadvertently used during testing instead of fictitious test data. 3. Risk of reputational association if the security testing tools and techniques used (OWASP ZAP, Burp Suite, SQLMap) were, through misconfiguration, directed at a University network resource or any system outside the isolated local test environment.	*How you will mitigate the risk to the University:* 1. All testing, findings, and exploitation techniques are confined strictly to a self-built, self-owned application within an isolated local environment, with no connection to any live, production, University, or third-party system at any stage. The dissertation will clearly state the controlled scope and isolated nature of the testing environment, and any discussion of vulnerabilities will be framed academically and defensively (i.e. focused on identification and remediation), consistent with standard responsible security-research practice. 2. Only fictitious, self-generated test data (invented names, test email addresses) is used throughout the project; no real personal, financial, or institutional data is collected, stored, or processed at any point. 3. All testing tools are configured and verified to target only the local test environment (confirmed via localhost/local VM network addresses) before each testing session, ensuring no University network, infrastructure, or third-party system is inadvertently scanned or targeted.
5	**Environmental risks** For example: accidental spillage of pollutants, damage to local ecosystems	
	Risk to the environment:	*How you will mitigate the risk to environment:*

	This research involves no fieldwork, chemical use, or physical materials, and is conducted entirely through desk-based technical work using a personal computer and virtualised software environments (XAMPP and a Kali Linux virtual machine). No direct environmental risks, such as pollutant spillage or damage to local ecosystems, are applicable to this project. The only identifiable environmental consideration is the electricity consumption associated with running a computer and virtual machine for extended periods during testing.	As the research involves no physical materials, chemicals, or fieldwork, no specific environmental mitigation measures are required beyond standard good practice. Electricity consumption is minimised by running the virtual machine only during active testing sessions and shutting down the test environment when not in use.

SECTION G: Feedback, Consent and Confidentiality

If you have identified in section D that there are no participants then enter skip this section and continue to section H.

1	**Feedback** What de-briefing and feedback will be provided to participants, how will this be done and when?
	You don't need to email your participants with your final report. A good alternative is to set up an email address that they will be able to contact for further details or results. N/A This research does not involve human participants; therefore, no participant de-briefing or feedback process is applicable. The only "feedback" arising from this project is academic in nature - the completed dissertation, documenting the vulnerabilities identified, the remediation applied, and the results of re-testing, will be submitted to my supervisor and assessed as part of the standard MSc dissertation evaluation process.
2	**Informed consent** Describe the arrangements to inform potential participants, before providing consent, of what is involved in participating. Describe the arrangements for participants to provide full consent before data collection begins. If gaining consent in this way is inappropriate, explain how consent will be obtained and recorded in accordance with prevailing data protection legislation.
	If you are using a paper questionnaire then you should have the participants sign an appropriate consent form. These forms will count as personal data and should be noted as such in section J. If you are using an online questionnaire, then you should have a screen before the questions start that acts as a consent form, informing participants that by clicking on the NEXT button they are providing consent. N/A This research does not involve human participants, and therefore no consent procedures are required. All testing is conducted solely against a system that I personally designed, built, and own, using fictitious test data created by myself. As no individuals are recruited, surveyed, interviewed, or otherwise involved as research subjects, informed consent procedures and associated documentation (e.g. participant information sheets, consent forms) are not applicable to this project.
3	**Confidentiality / Anonymity** Set out how anonymity of participants and confidentiality will be ensured in any outputs. If anonymity is not being offered, explain why this is the case.
	Do not collect names unless you really need them. Do not name participants or organisations in any research publications (including the thesis) without their explicit permission. N/A This research does not involve human participants, and no personal data belonging to real individuals is collected, processed, or stored at any point. All test accounts (customer and administrator) used during security testing are fictitious, created solely by myself using invented names and test email addresses for the purpose of this project. As there are no participants and no real personal data involved, questions of anonymity and confidentiality of participants do not apply to this research.

SECTION H: Data Protection and Storage

	Does the research activity involve personal data (as defined by the General Data Protection Regulation 2016 "GDPR" and the Data Protection Act 2018 "DPA")?	YES	NO
1	***"Personal data"*** *means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Any video or audio recordings of participants is considered to be personal data.*	☐	☐
	If YES, provide a description of the data and explain why this data needs to be collected:		
2	This includes audio/video data of participants, but can also include IP addresses and usernames. Names, addresses and emails also count, as do consent forms. *(this box should expand as you type)*		
	Does it involve special category data (as defined by the GDPR)?	YES	NO
3	***"Special category data"*** *means sensitive personal data consisting of information as to the data subjects' –* *(a) racial or ethnic origin,* *(b) political opinions,* *(c) religious beliefs or other beliefs of a similar nature,* *(d) membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),* *(e) physical or mental health or condition,* *(f) sexual life,* *(g) genetics,* *(h) biometric data (as used for ID purposes),*	☐	☒
	If YES, provide a description of the special category data and explain why this data needs to be collected:		
4	What counts as 'sensitive' will differ between cultures. Any information on behaviour that is not in accordance with cultural norms would count as sensitive personal data. N/A This research does not collect, process, or store any special category or sensitive personal data. No human participants are involved, and all data used during testing (customer and administrator accounts) is entirely fictitious, created solely by myself for the purpose of populating the self-built test application. No real individuals' personal, behavioural, health, financial, or otherwise sensitive information is collected at any stage of this project.		

	Will data from the research activity (collected data, drafts of the thesis, or materials for publication) be stored in any of the following ways?	YES	NO
5	Manual files (i.e. in paper form)?	☐	☒
6	University computers?	☒	☐
7	Private company computers?	☐	☒
8	Home or other personal computers?	☒	☐
9	Laptop computers/ CDs/ Portable disk-drives/ memory sticks?	☒	☐

10	"Cloud" storage or websites?	☒	☐
11	Other – specify:	☐	☒
12	For all stored data, explain the measures in place to ensure the security of the data collected, data confidentiality, including details of backup procedures, password protection, encryption, anonymisation and pseudonymisation:		
	If possible, save your data on computers that are secure and regularly backed up. Many cloud services only provide GDPR-compliant storage for business customers. An example of suitable text is given below. All data generated during this research (scan logs, captured HTTP requests, screenshots, database records) relates solely to a self-built test application populated with fictitious test data, and is stored locally on my own personal computer within password-protected user accounts. No real personal or third-party data is collected, so anonymisation and pseudonymisation are not applicable, as all test data (names, emails, card numbers) is invented rather than derived from real individuals. The test environment itself incorporates several security measures consistent with the project's own findings: database credentials are stored in a separate configuration file outside the web-accessible directory rather than hard-coded, the database is accessed through a dedicated least-privilege account rather than a shared administrative one, and passwords within the test application are stored using bcrypt hashing rather than in plain text. Regular local backups of the test database and virtual machine are taken before higher-risk testing (e.g. concurrent-request testing), allowing the environment to be restored if disrupted. All project documentation, screenshots, and the dissertation itself are stored on my personal, password-protected computer and backed up to a private, access-controlled cloud storage account. No data collected during this project is shared with or accessible to any third party.		

	Data Protection		
	Will the research activity involve any of the following activities:	**YES**	**NO**
13	Electronic transfer of data in any form?	☒	☐
14	Sharing of data with others at the University outside of the immediate research team?	☐	☒
15	Sharing of data with other organisations?	☐	☒
16	Export of data outside the UK or importing of data from outside the UK?	☒	☐
17	Use of personal addresses, postcodes, faxes, emails or telephone numbers?	☐	☒
18	Publication of data that might allow identification of individuals?	☐	☒
19	If YES to any question, please provide full details, explaining how this will be conducted in accordance with the GDPR and Data Protection Act (2018) (and/or any international equivalent):		
	N/A - No personal data belonging to real individuals is collected as part of this research, and therefore no GDPR/Data Protection Act 2018 obligations arise in relation to participant data, as there are no participants. For completeness, the technical and dissertation data generated during this project (test logs, screenshots, draft chapters) will be stored and protected as follows: all data will be kept in password-protected storage on my personal computer and backed up to a private, password-protected cloud storage account which will not be shared with any third party. Any external storage media (e.g. USB drives) used to transfer or back up this data will be password protected. As no real participants or personal data are involved, no unique participant identifiers are required. The data will be retained until completion and assessment of the project, after which it will be deleted in line with standard good practice for the secure disposal of dissertation working data.		
20	List all who will have access to the data generated by the research activity:		

	Access to the data generated by this research (test logs, screenshots, database records, dissertation drafts) will be limited to: 1. **Myself (the researcher)** - as the sole individual conducting the testing and holding administrative access to the local test environment and stored data. 2. **My project supervisor** - for the purposes of reviewing progress, providing guidance, and assessing the completed dissertation. 3. **Assessors/examiners at the University** - for the purposes of marking and moderating the dissertation as part of the standard MSc assessment process. No other individuals or third parties will have access to the data, as all testing is conducted on a self-built, self-owned system containing no real personal or third-party data.	
21	List who will have control of, and act as custodian(s) for, data generated by the research activity:	
	I, as the researcher, will act as the sole custodian of all data generated by this research activity, retaining full control over the storage, security, and eventual disposal of the test logs, screenshots, database records, and dissertation drafts produced during the project. As no external participants, third-party organisations, or shared datasets are involved, no joint or external data custodianship arrangements are required.	
22	Give details of data storage arrangements, including security measures in place to protect the data, where data will be stored, how long for, and in what form.	
	All data generated during this research (scan logs, captured HTTP requests, screenshots, database exports, and dissertation drafts) will be stored locally on my personal computer within a password-protected user account, with regular backups made to a private, password-protected cloud storage account that is not shared with any third party. Data will be stored in its native technical form: log files and scan reports (text/HTML/PDF formats generated by OWASP ZAP, Nikto and SQLMap), captured request/response data and screenshots (PNG/JPEG image files) from Burp Suite and browser testing, database exports (SQL format) from phpMyAdmin, and dissertation chapters (Word document format). As no real personal or third-party data is involved, encryption of participant identities and anonymisation procedures are not applicable; however, standard security good practice is followed throughout - the storage device and cloud account are both password protected, and the test application's own database credentials are kept outside the web-accessible directory rather than hard-coded. Data will be retained until the completion, submission, and final assessment of the dissertation, after which it will be securely deleted from both local and cloud storage, in line with standard good practice for the disposal of academic project working data. No data is retained beyond this point, as it holds no further research or personal value once the project has been assessed.	
22	Confirm that you have read the UWTSD guidance on data management (see https://www.uwtsd.ac.uk/library/research-data-management/)	☒
23	Confirm that you are aware that you need to keep all data until after your research has completed or the end of your funding	☒

SECTION I: Use of AI tools

Use of generative AI and other AI-based tools There are a number of ethical issues relating to the use of generative AI and other AI-based tools, including data security, output bias, and output errors. In general you should assume that any generative AI or other AI-based tool that you pay to use is more secure and accurate than one which is free to use. Will the research use AI tools to do any of the following:	**YES**	**NO**	**N/A**

1	Capture data?	☐	☒	☐
2	Generate and/or edit text?	☐	☒	☐
3	Generate graphics?	☐	☒	☐
4	Generate video?	☐	☒	☐
5	Generate sound/music?	☐	☒	☐
6	Generate code?	☐	☒	☐
7	Generate synthetic data?	☐	☒	☐
8	Analyse data?	☐	☒	☐
9	Analyse personal or sensitive data?	☐	☒	☐
10	Classify data?	☐	☒	☐
11	Do you intend to use the free version of any AI tools?	☐	☒	☐
If you have answered **YES** to any of questions O1-O11, please provide justification detailing why this is necessary for the research.				
12	N/A I have not answered "Yes" to any of questions O1-O11, as this research does not involve human participants, vulnerable groups, deception, incentives, invasive procedures, or any of the higher-risk research categories these questions typically address. This project is a purely technical Vulnerability Assessment and Penetration Testing exercise conducted against a self-developed application within an isolated local environment, using only fictitious test data created by myself. As no applicable "Yes" responses arise, no further justification is required for this section.			

SECTION J: Declaration

	The information which I have provided is correct and complete to the best of my knowledge. I have attempted to identify any risks and issues related to the research activity and acknowledge my obligations and the rights of the participants. In submitting this application I hereby confirm that I undertake to ensure that the above named research activity will meet the University's Research Ethics and Integrity Code of Practice which is published on the website: https://www.uwtsd.ac.uk/research/research-ethics/		
1	**Signature of applicant:**	Jay Shaileshbhai Lad	**Date:** 24-09-2026
2	Supervisor:	Fahed Ahmed	**Date:**
3	Signature:		