Council Dog Infrastructure Model

Owner: The Council
Reviewer: SENG406 Teaching Team
Contributors: Isla Smyth, Campbell Shephard, Chloe McLaren, Daniel Lowe
Date Generated: Fri Aug 16 2024

Executive Summary

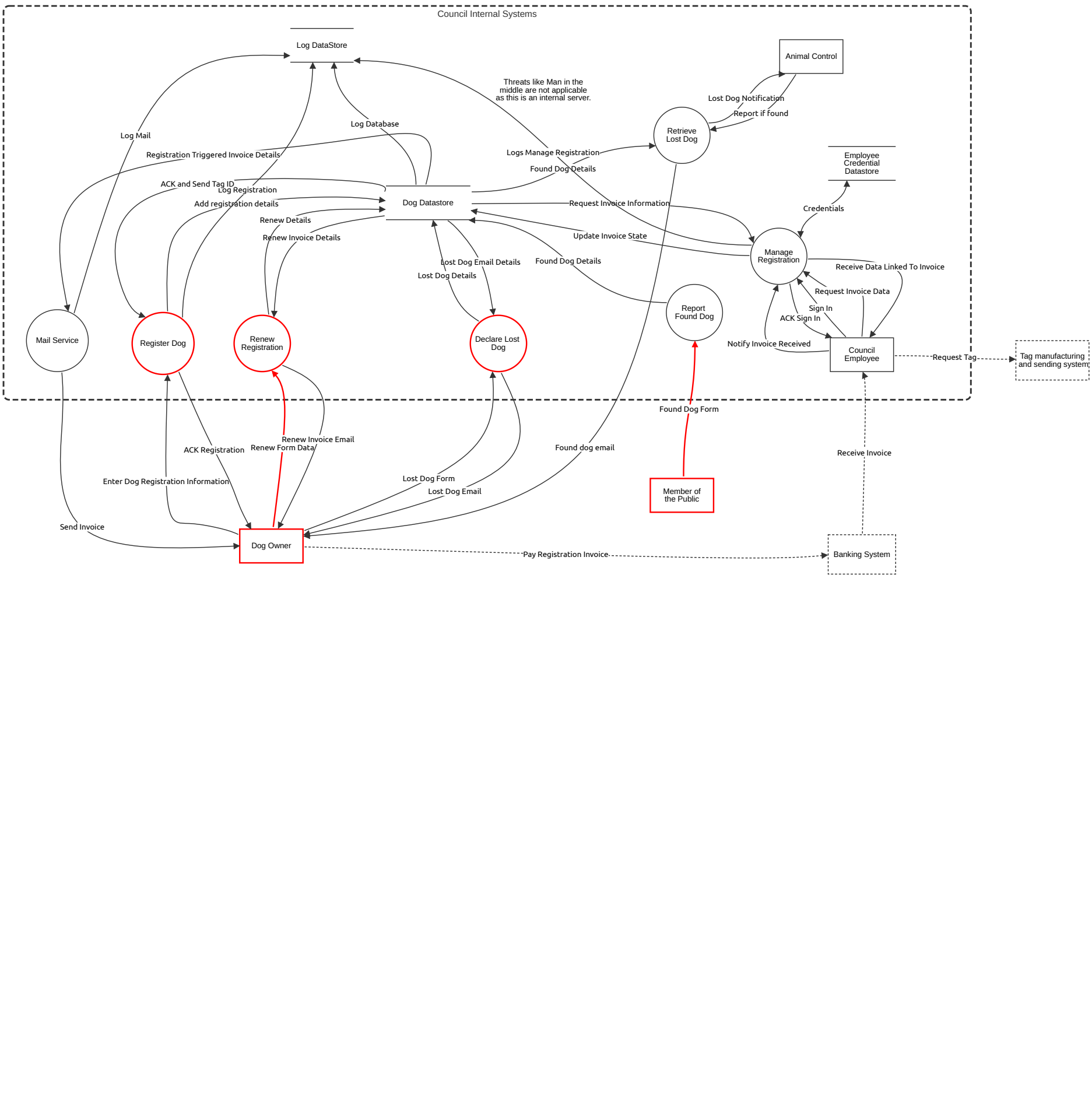
High level system description

Threat Dragon model for the Council Dog Registration

Summary

Total Threats	62
Total Mitigated	52
Not Mitigated	10
Open / High Priority	0
Open / Medium Priority	7
Open / Low Priority	3
Open / Unknown Priority	0

Main Diagram



Main Diagram

Dog Owner (Actor)

A person who legally owns one or more dogs and is in the council's range of authority, so wants to register their dog or manage their already existing regulations.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
127	Incorrect Details	Spoofing	Medium	Open		Users could provide incorrect details, such as an incorrect email, address or dog information.	Require email verification. Validate addresses syntactically and through a location API.

Register Dog (Process)

HTTPS web page endpoint(s) and api(s) that are used for dog registration.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	Fake Information	Spoofing	Medium	Open		Someone could enter fake information, meaning the authorities no longer know who owns the dog, or if the dog even exists.	(Not implemented) - Use a system like Real Me to verify the person's identity. - Make people send a photo of themself holding photo ID - Check the email address/physical address are legitimate (filter for common fake subdomains)
13	Claim against Registration	Repudiation	Low	Mitigated		Owner performs registration, then claims they didn't register any such dog.	- Log all registration actions to the system. Include relevant information about the request, i.e., IP address, time/date
36	Website spoofing	Spoofing	Medium	Mitigated		Someone could create a fake version of this website, causing people to give their information to the wrong people.	- Prioritise shorter URLs - Purchase and redirect from similar domains
116	Denial of service	Denial of service	Medium	Mitigated		Someone could flood the end point with fake applications, which causes real applications to be missed as it overwhelms the server.	Rate limit the endpoint Have a white list for allowed requests.

Dog Datastore (Store)

Stores information relating to dog entities known under the council.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
20	Database Injection	Tampering	High	Mitigated		Injection attacks could be used to change the database's information.	- Follow industry practices for sanitising input - Ensure all libraries used are up-to-date and screened for CSE vulnerabilities - Create frequent backups of the database and store them externally
24	Disclosure by Injection	Information disclosure	Medium	Mitigated		Injection attacks could be used to get information.	- Follow industry practices for sanitising input - Ensure all libraries used are up-to-date and screened for CSE vulnerabilities
25	Flooding Attack	Denial of service	Low	Mitigated		Too many requests in a short amount of time could overwhelm the data store and cause it to stop.	Rate limit interactions with the datastore.
50	Unauthorized Database Access	Information disclosure	Medium	Mitigated		If an attacker gains access to the database, then they could view all the information in the database easily.	Hash all user information by the generated tag ID so that user information can only be received if you have the tag ID.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
117	Repudiation	Repudiation	Medium	Mitigated		Someone could make a change or update to the database and claim that they did not in the future.	Log all requests with the database.

Renew Invoice Details (Data Flow)

Contains details pertinent to the renew registration email invoice that were not obtained in the web form process: full name, pronouns, registration number, and email address.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Renew Details (Data Flow)

Contains both the old and new tag IDs, the new physical address, and a new expiry date. Sets the flag is_paid to false.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Sign In (Data Flow)

Council credentials, including email and password.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

ACK Sign In (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Lost Dog Email (Data Flow)

Confirmation email for a lost dog declaration, confirming the dog's last known tag ID.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
65	Intercepted email	Information disclosure	Medium	Mitigated		Email could be intercepted and user information could be gained.	Ensure that email is sent over a secure connection using TLS and have checksums.
66	Modified email	Tampering	Medium	Mitigated		Email could be modified to add incorrect information or fake links.	Ensure that email is sent over a secure connection using TLS and have checksums.

Request Tag (Data Flow) - *Out of Scope*

The council employee manually requests the tags to be made and shipped to the address that the invoice is related to.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Found Dog Details (Data Flow)

Contains the dog's tag ID, current status, and possibly the reported sighting address.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Found Dog Details (Data Flow)

Information necessary for animal control to find and return dog.
Last address of dog, dog tag ID, dog breed, owner’s address

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request Invoice Information (Data Flow)

The information for the provided reference that is required to send the tag is retrieved, so the dog ID and the address.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Update Invoice State (Data Flow)

The invoice is marked as paid for the provided reference.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Credentials (Data Flow)

Employee credentials (i.e., email/password)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Add registration details (Data Flow)

Contains all of the details from the registration form: the human pronoun, first and last name, email address, and physical address, and the dog's name and breed. This information is used to create a new entry in the database.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Logs Manage Registration (Data Flow)

Contains all actions taken while managing the registration.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Log Database (Data Flow)

Logs every request to the database

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Log Registration (Data Flow)

Logs all registrations or attempts at registration

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Log Mail (Data Flow)

Logs all requests to send mail and all mail that is sent

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Pay Registration Invoice (Data Flow) *- Out of Scope*

The dog owner pays for the invoice from their registration with the details listed in the invoice.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Receive Invoice (Data Flow) *- Out of Scope*

Council employees check that the bank transfers made to the assacated bank account.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Receive Data Linked To Invoice (Data Flow)

The employee receives the data linked to the reqeasted invoice so that they can create and send a tag, so the address and the dog id

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request Invoice Data (Data Flow)

The employee enters the invoice reference to find information about the linked dog owner so that they can create and send the tag.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

ACK and Send Tag ID (Data Flow)

acknowledges that a regulation was successful and gets the generated unique dog ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Notify Invoice Received (Data Flow)

The employee notifies the system that they have sent the tag and that the invoice is now paid by providing the invoice refrance.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Registration Triggered Invoice Details (Data Flow)

Once registration details have been updated, invoice details are generated in the database and sent to the mail service.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Lost Dog Notification (Data Flow)

Notifies animal control about lost dogs and any information on them.
(reported address of dog, tag ID, breed, and dog name)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
134	Violation of Least-Privilege	Information disclosure	Medium	Mitigated		Information could be sent to more people in animal control than just the individuals directly responsible for investigating the report.	Allocate and send notifications only to specific animal control employees.
135	Flooded with fake notifications	Denial of service	Medium	Mitigated		Too many false notifications of found dogs will overwhelm animal control, and prevent them from checking for missing dogs.	Disallow multiple requests from the same origin IP (IP blocking after multiple calls) within a few seconds. Disallow requests not from known IPs (such as the council) Block IPs from known attackers. Limit the amount a dog can be lost to once an hour.
136	Man in the middle	Tampering	Medium	Mitigated		Man in the middle attack could be performed on the notification if there is an insecure connection, allowing for information sent to animal control to be modified.	Ensure that HTTPS is used to encrypt the data. Verify a dog with the given ID exists and is lost. Verify the last address of the dog is within a reasonable distance of the owner's address. Verify the identity of the owner when returning the dog. Encrypt information.
137	Notification details publicly accessible	Information disclosure	Medium	Mitigated		Malicious actor could intercept information such as dog details, dog location, owner’s address, etc.	Use a secure transfer protocol. Encrypt information.

Report if found (Data Flow)

Form for reporting if the dog was found at the stated address or not. Includes the tag ID of the dog in question, and a flag for if it was found at the address or not.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
139	False Report	Tampering	Medium	Mitigated		A malicious animal control employee could wrongly claim that a dog has been found, or (more likely) wrongly claim a dog wasn't found.	Animal control employees should work in small groups, and their vehicles should be GPS monitored.
141	Man in the Middle	Tampering	Medium	Mitigated		Man in the middle could tamper with data to report a dog was/wasn't found.	Ensure that HTTPS is used to encrypt the data. Use hashing to check if data has been modified.

Found dog email (Data Flow)

Notify owner that their dog has been found.
Contains: Dog tag ID and last known location, owner’s email address and other personal details.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
113	Adversary in the middle	Tampering	Medium	Mitigated		An adversary-in-the-middle intercepts the email and modifies its content or blocks/redirects sending.	Use a secure email transfer protocol
114	Details publicly accessible	Information disclosure	Medium	Mitigated		Email could be intercepted and personal information could be obtained such as name, address, dog location, etc.	Minimize personal details in email, especially addresses (could have generic message like ‘Your dog has been found!’). Use secure transfer protocol.

Renew Form Data (Data Flow)

Form consisting of dog's tag ID and new delivery address.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
83	Data Tampering	Tampering	Medium	Mitigated		A man-in-the-middle attacker could tamper with the form data, altering the physical address field to send it to.	Use HTTPS to encrypt the form data, and send the form data with a generated hash to ensure it hasn't been tampered.
84	Data interception	Tampering	Low	Mitigated		An attacker could intercept the data sent, obtaining the sender's physical address and tag ID.	Use HTTPS to encrypt the data.
85	Flooding Attack	Tampering	Medium	Open		An attacker could flood the renew registration page with illegitimate form requests, denying its use by legitimate actors.	Rate limit the number of form requests accepted per IP address. Implement a captcha test before forms can be sent. Filter requests upstream using an external protection service, such as Amazon Shield or Cloudflare to check packets against known attacker addresses.
122	Injection Attack	Tampering	High	Mitigated		Attacks such as SQL or code injection could be used to perform unauthorised actions on the datastore through the form fields.	Parameterise and sanitise the form fields to ensure any text within them isn't treated as executable.

Renew Invoice Email (Data Flow)

Personalised email addressed to the owner, with invoice attached as a PDF.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
92	Interception of Data	Information disclosure	Medium	Mitigated		Email could be intercepted by an attacker, granting them access to the registration owner's pronouns, full name, and email address.	Ensure the email is sent via TLS.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
93	Man-in-the-Middle Attack	Tampering	Medium	Mitigated		Data could be tampered with via a man-in-the-middle attack, altering the invoice details, such as amount owed, or the bank account (i.e., if the invoice contains the account number, the number could be altered. If the invoice or email instead contains instructions on where to find the account number, these instructions could be altered, perhaps to point to a spoofed website). The PDF could also be altered to contain malicious executable code.	Ensure the email is sent via TLS.

Enter Dog Registration Information (Data Flow)

Enters the information for registering a dog.
the human pronoun, first and last name, email address, and physical address, and the dog's name and breed. This information is used to create a new entry in the database.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	Man in the middle Tampering	Tampering	High	Mitigated		Someone could do a man-in-the middle attack and view and manipulate the data while it is in transit.	By using HTTPS this is prevented as the data is encrypted in transit so they could only do this if they got the data from the connection at the very start.
9	Man in the middle, spying	Information disclosure	Medium	Mitigated		Someone could be a man in the middle and spy on people using the application, therefore getting information like their address and email	By using HTTPS, someone would need to see the start of the communication to be able to intercept the communication.

ACK Registration (Data Flow)

Acknowledges that the registration was successful, and informs the owner of the registration number and expiry date for the registration.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
10	Spying	Information disclosure	Low	Mitigated		some one could spy on the infomation while it is in transit.	By using HTTPS, someone would need to see the start of the communication to be able to intercept the communication.
56	Tampering	Tampering	Medium	Mitigated		Acknowledgement could be tampered with; i.e., changing registration number to another registration. Since this is used in the reference for a bank transfer, the owner could end up failing to pay their own registration.	Use HTTPS

Send Invoice (Data Flow)

An invoice is generated and mailed to the dog owner.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
42	Man in the middle Infomation disclosure	Information disclosure	Medium	Mitigated		Someone could be a man in the middle and spy on people using the application for getting information like their address and email.	All emails would be encrypted, so this information could not be disclosed.
43	Man in the middle Tampering	Tampering	Medium	Mitigated		Someone could be a man in the middle and change information in the invoices so that the invoice is instead sent to them.	All emails would be encrypted, so the emails can't be changed and produce meaningful data.

Lost Dog Email Details (Data Flow)

Contains the dog's tag ID, along with details for email personalisation -- owner's full name and pronouns.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Lost Dog Details (Data Flow)

Contains the owner's email address, dog's name, and status to update to.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Lost Dog Form (Data Flow)

Form consisting of the owner's email address and dog's name.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
63	Flood of fake form requests	Denial of service	Medium	Mitigated		If too many fake form requests are made the servers could get overwhelmed and limit actual users.	Rate limit the number of form requests per user IP. Limit the amount a dog can be lost to once an hour.
64	Man in the middle attack	Tampering	Medium	Mitigated		Form data could be altered with a man in the middle attack allowing for wrong information of dog being lost or for code to be added into the form.	Ensure that HTTPS is used to encrypt the data.

Found Dog Form (Data Flow)

Contains: Last address of dog, dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations
109	Insecure connection/Adversary in the middle	Tampering	Medium	Mitigated		An adversary-in-the-middle intercepts the form and modifies its content. (Change location or dog tag ID)	Use Transport Layer Security for the communication Use secure connection, https-only and secure cookie with unique session id. Add encryption/checksums to information.
110	Address publicly accessible	Information disclosure	Medium	Mitigated		When submitting a form, the current location of the member of the public or the dog could be visible to anyone.	Use a secure transfer protocol. Encrypt information.
111	Flooding of forms	Denial of service	Medium	Open		More than one found dog form coming from the same user within a few seconds.	Disallow multiple requests from the same origin IP (IP blocking after multiple calls) within a few seconds. Block IPs from known attackers. Implement Captcha system.

Renew Registration (Process)

HTTPS webpage endpoint(s) for renewing a dog's registration.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
86	Website Spoofing	Spoofing	Medium	Open		Someone could create a fake version of this website, causing people to give their information to the wrong people.	- Prioritise shorter URLs - Purchase and redirect from similar domains
87	False Information	Spoofing	Low	Open		Users could provide incorrect renewal details, such as an invalid address.	Validate addresses syntactically and through a location API.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
88	Claim against renewal	Repudiation	Low	Open		Owners could claim they hadn't performed a registration renewal when they had.	- Log all renewal actions to the system. Include relevant information about the request, i.e., IP address, time/date
89	Data Interception	Information disclosure	Medium	Mitigated		An attacker could intercept the data sent, obtaining the sender's physical address and tag ID.	Use HTTPS to encrypt the data.
90	Data Tampering	Tampering	Medium	Mitigated		A man-in-the-middle attacker could tamper with the form data, altering the physical address field to send it to.	Use HTTPS to encrypt the form data, and send the form data with a generated hash to ensure it hasn't been tampered.
91	Flooding Attack	Denial of service	Medium	Open		An attacker could flood the renew registration page with illegitimate form requests, denying its use by legitimate actors.	Rate limit the number of form requests accepted per IP address. Implement a captcha test before forms can be sent. Filter requests upstream using an external protection service, such as Amazon Shield or Cloudflare to check packets against known attacker addresses.

Declare Lost Dog (Process)

HTTPS webpage endpoint(s) for declaring a dog as lost.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
67	Fake dog owner	Spoofing	Medium	Open		Someone else fills a fake form that a dog has been lost.	Have a login system for dog owners.
68	Inserted code	Tampering	Medium	Mitigated		Code could be inserted into the form for the server to run.	Check the form inputs for any code.
69	Claim against reporting lost	Repudiation	Medium	Mitigated		Declares a dog lost and then claims later that they did not.	To log the IP date and time when someone claims a dog lost.
70	Too many requests	Denial of service	Medium	Mitigated		If too many requests are sent then the servers get overwhelmed and not be able to handle more lost dogs.	Rate limit the number of form requests per user IP. Limit the amount a dog can be lost to once an hour.

Report Found Dog (Process)

HTTP webpage endpoint(s) for reporting a dog as found.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
78	Fake information	Spoofing	Medium	Mitigated		Someone gives fake information about a found dog	Check for a real address. Log who makes claims and blacklist multiple fake reports.
79	Inserted code	Tampering	Medium	Mitigated		Code could be inserted into the form for the server to run.	Check the form inputs for any code.
80	Claim against finding dog	Repudiation	Medium	Mitigated		Claims they did not make a report for finding a dog.	To log the IP date and time when someone claims to find a dog lost.

Member of the Public (Actor)

Members of the public can report lost dogs they have found.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
105	Incorrect input	Spoofing	Low	Open		Member of the public inputs incorrect dog tag or address (intentionally or unintentionally)	(Not implemented) Use location data from the user's device to determine address. Require a photo of the dog tag. Check if the tag with that id exists. Ignore if the dog tag id is not lost within a reasonable distance of the owner's address. Check address is valid.

Council Employee (Actor)

A person who works for the company in an admin role for the system.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
81	Staff credentials could be stolen or guessed	Spoofing	High	Mitigated		Someone could obtain or guess the credentials of a council employee, gaining access to the system when they shouldn't.	Enforce strong password rules (for length and character types, i.e., special characters). Block the use of common passwords and phrases. Require two-factor authentication for logging in. Periodically enforce changing passwords, and disallow the use of previous passwords. Automatically expire user sessions after a period of inactivity (i.e., 30 minutes), and after a total elapsed period (i.e., 8 hours). Consider funding and distributing to staff members an external password service, and educate about its usage.
82	Staff member modifies a registration and claims otherwise	Repudiation	Medium	Mitigated		A staff member with valid credentials could modify a dog's registration in the data store, then claim they didn't modify it.	Log all database transactions and employee logins to a file. Include the details of any transaction performed, along with other relevant information, such as the user who performed it and the time and date it occurred.

Manage Registration (Process)

Council-only end-point for viewing and manipulating the dog registration datastore directly.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
47	Insider Spying	Information disclosure	Medium	Mitigated		A concil employee could get the personal information of people in the system for their own use e.g., they could get their X address if they have a dog and know some of their personal information.	To request customer data, they need to use the invoice registration number, and only the address and the tag ID will be returned. All actions by the employee are also recorded so that any malicious activity can be found, such as spamming possible dog tags.
118	Insider Tampering	Tampering	Low	Mitigated		Someone could falsely claim that someone they know has paid for a tag when they have not.	All actions are logged, and work is checked over by other employees.

Employee Credential Datastore (Store)

Stores all council employee credentials.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Mail Service (Process)

Used to send mail.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
34	Denial of Service	Denial of service	Medium	Mitigated		Too many mail requests could be made that cause the system to only send some of them.	Rate limit intraction with the emailer and keep a stack of all the emails that still need to be sent.
115	Fake Invoice	Spoofing	High	Mitigated		An attacker could create a fake invoice in the same style as the real invoices and send them to customers they know are getting dogs and are in the area, so that they can steal money from them.	The invoices would contain all the information you entered about you and your dog, including the random ID, which the registration form will ask the user to keep for this purpose, so that to accurately fake an invoice, the attacker would have to have access to the database. Well, in the likely case that a user forgot their tag ID, they would still need their other information, to create a convincing invoice. But most people would still be tricked by an official looking invoice even if it was not perfect. The problem still persists as most of this data would be publicly available other than the tag ID, which they are likely to forget.

Banking System (Actor) *- Out of Scope*

Used to transfer money between accounts so that money can be paid

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Tag manufacturing and sending system (Actor) *- Out of Scope*

The system for creating and sending the tags to dog owners

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Retrieve Lost Dog (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Animal Control (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
73	Fake user	Spoofing	Medium	Mitigated		Another person gains access to a animal controllers account	Implement a multifactor login system Enforce strong password polices
74	False claims	Repudiation	Medium	Mitigated		Claim that a dog has been collected when it has not been. Or claim a dog is still missing when it has been found.	Log when user signs in and out and what they interact with.

Log Datastore (Store)

Stores all logs for the system

Number	Title	Type	Priority	Status	Score	Description	Mitigations
130	Injection Tampering	Tampering	Medium	Mitigated		Injection attacks could be used to change the database's information.	- Follow industry practices for sanitising input - Ensure all libraries used are up-to-date and screened for CSE vulnerabilities - Create frequent backups of the database and store them externally
120	Disclosure by Injection	Information disclosure	Medium	Mitigated		Injection attacks could be used to get information.	- Follow industry practices for sanitising input - Ensure all libraries used are up-to-date and screened for CSE vulnerabilities - The log datastore dose not send infomation anywhere other then to admin staff
121	Repudiation by Injection	Repudiation	Medium	Mitigated		Injection attacks could be used to destroy logs or prevent them form forming by making them contain	- Follow industry practices for sanitising input - Ensure all libraries used are up-to-date and screened for CSE vulnerabilities - even if a log can't be saved, record that an unsantizeable log was made and it's original.