SENG406 Assignment 2

Daniel Lowe
Department of Software Engineering
University of Canterbury
Christchurch, New Zealand
dlo54@uclive.ac.nz

Chloe McLaren
Department of Electrical and Computer Engineering
University of Canterbury
Christchurch, New Zealand
cmc335@uclive.ac.nz

Isla Smyth
Department of Software Engineering
University of Canterbury
Christchurch, New Zealand
irs28@uclive.ac.nz

Campbell Shepherd
Department of Electrical and Computer Engineering
University of Canterbury
Christchurch, New Zealand
csh113@uclive.ac.nz

I. Lists

A. Actors

ID	Actor Name	Description
U1	Dog Owners	People who own dogs and either want to register or have registered a dog
U2	Members of the Public	People who report found dogs
U3	Animal Control	Receives requests to collect lost dogs
U4	Council Admin Staff	People who control the system.

B. Assumptions

ID	**Description**	**Justification**
S1	There is no user account registration system currently in place. Users are only validated by comparing the input form fields against existing registration fields.	There is no mention in the brief, and this a similar implementation to the Christchurch City Council's registration form.
S2	The council only contacts owners about a found dog report if the report resulted in animal control successfully finding the dog.	It wouldn't make sense to contact owners about potentially-false reports.
S3	Council admin staff access council services through an employee portal with appropriate login credentials, such as an email and password.	This reflects typical real-world practices for businesses.
S4	The service in the system responsible for sending emails cannot receive emails.	This reflects many real-world institutional email addresses, which are no-reply.
S5	Bank transfers and tag shipping requests are manually reviewed and enacted by council employees.	Manual verification is plausible here, though either implementation would have similar risks.
S6	The council internal system (trust boundary) does not interact with the outside world or internet beyond the specified cases.	This reflects many workplace intranet setups, and makes the system more secure.
S7	The council internal system employs parameterisation of form input to mitigate against injection attacks	This reflects typical industry best-practices.
S8	The council internal system employs logging of employee and database transactions.	This reflects typical industry best-practices.
S9	Generated unique registration numbers are realistically complex (i.e., ten or more digits in length), and not easily guessed (i.e., "1").	Most registration systems operate under this assumption in the real world.

C. Constraints

ID	Description
C1	The system must be available publicly on a website from both desktop and mobile devices.
C2	The full software application is deployed on premise, controlled by the Council's staff.
C3	Council staff maintain the infrastructure (hardware) that runs the software application.
C4	All personal details should be kept private, especially physical address, email address, and payment information.
C5	All emails and invoices are sent and replied to within 3 working days.
C6	Tags are shipped after payment is received within 5 working days.
C7	Lost dog information is priority-updated within the hour.
C8	Dog's physical addresses must be a real addresses.
C9	Adhere to all relevant laws.
C10	Registrations can only be renewed within or after the last month of their duration.

D. Dependencies

ID	Name	Description
D1	Banking System.	The system that is used to transfer money between accounts is used in the system to transfer money for payment.
D2	Dog Tag Manufacturer.	The people who manufacture the dog tags are used to manufacture the dog tags so that they can be delivered to the appropriate people.
D3	Snail Mail Service.	The mail service that sends physical packages around is used to send the dog tags to the dog owners
D4	Internet.	The system used to communicate information around the world. Is used so that dog owners and members of the public can interact with the system.
D5	Council Infrastructure.	The infrastructure that the council uses to run this program (the servers they own and operate)
D6	Third-party software used.	All third party software used by the system.
D7	Third-party hardware used.	All third party hardware used by the system.

E. Trust Levels

ID	Level	Actors	Permissions Granted
T1	2	U4 (Council Admin Staff)	Can view the registration database, view received transactions for the council bank account, and send emails from the internal council address.
T2	1	U3 (Animal Control)	Can view the dog's tag ID, dog name, dog breed, and reported address information from registrations where the dog's status is "FOUND".
T3	0	U1 (Dog Owners), U2 (Members of the Public)	Can post form information to the available council entry-points.

F. Entry Points

ID	Name	Description	Trust Levels
E1	Registration Form	HTTPS form for registering a dog. Allows for inputting a pronoun, first/last names, email address, physical address, dog name, and dog breed.	0
E2	Renew Form	HTTPS form for renewing a dog's registration. Allows for inputting a dog's existing tag ID and the new delivery address.	0
E3	Receive Invoice	Council employees check that the bank transfers made to the associated bank account.	2
E4	Lost Dog Form	Enters the information for declaring an owners dog lost. The owners email address, dog name, dog registration number, and the possible address. Relevant information from the matched registration is then sent to animal control.	0
E5	Found Dog Form	Form for inputting location and dog tag ID of a suspected lost dog.	0
E6	Terminate Registration Form	Form for termination registration of a dog, requires the email address, dog's name and dog tag ID linked to that dog. Sends a confirmation email on completion with a link to the registration form.	0
E7	Retrieve Lost Dog	Page for viewing reports of found dogs. Displays the dog's tag ID, name, breed, and reported address. Also has a form for reporting if the dog is successfully found at the reported location or not.	1

G. Exit points

ID	Name	Description
X1	ACK registration	acknowledges that the registration was successful, and informs the owner of the registration number and expiry date for the registration.
X2	Send Invoice	An invoice is generated and mailed to the dog owner.
X3	Request Tag	The council employee manually requests the tags to be made and shipped to the address that the invoice is related to.
X4	ACK Lost Dog	An email is sent to the owner to acknowledge that they confirm that their dog is lost and animal control will begin to start searching for the dog.
X5	Renew Invoice Email	Email sent to an owner after a successful Renew Registration request. Contains expected email personalisation (i.e., Owner's name and pronouns), instructions on how to pay for the renewed registration, and an attached PDF invoice.
X6	Found Dog Email	Email sent to an owner when their lost dog is successfully found, notifying them as such.
X7	Termination Email	Email sent to an owner after terminating their registration, containing a link to re-register.

H. Assets

ID	Name	Description
A1	Personal details	The pronouns, first/last names, email address, and physical address of people in the system.
A2	Dog information	The dog name, dog breed, registration number, tag ID, dog status, registration expiry date, and payment status of dogs in the system.
A3	Server logs	The logs of all actions taken in the system.
A4	Physical hardware	The hardware that the server and database run on.
A5	Software/source	The code used to run the system.
A6	Employee credentials	Stored details for the council employee, such as pronouns, first/last names, phone number(s), email address, physical address, next-of-kin and next-of-kin contact details, job description, salary information, along with their system credentials, including an encrypted password.

II. Functional Changes & Threat Analysis

A. Switching to a login-based authentication model.

1) Reason: There are multiple reasons that the current login-less system is not secure. For one, you can easily terminate or report as lost someone else's dog registration by knowing the person's email and having access to the dog to determine its name (collars often have names) and tag ID, which could cause a person to lose money as they have to re-register their dog. Can easily trick people into paying the wrong invoice by sending a fake invoice at around the same time they are registering a dog, though the email, in addition, has no way of verifying that the person registering a dog is who they say they are. By adding a login to the system, a lot of these issues can be fixed with minimal added risks.

2) Dependencies:

ID	Name	Description
D8	Telephone System	Phone resources to perform 2FA authentication requests.
D9	RealMe System	The NZ digital ID service.

3) Assets:

ID	Type	Name	Description
A1	Modified	Personal details	Now includes the corresponding RealMe account credentials: their username, encrypted password, and phone number.

4) Trust Levels:

ID	Level	Actors	Actions that they can take
T1	4	U4 (Council Admin Staff)	Can view the registration database, view received transactions for the council bank account, and send emails from the internal council address.
T2	3	U3 (Animal Control)	Can view the dog's tag ID, dog name, and dog breed information from registrations where the dog's status is "LOST".
T5	2	U1 (Dog Owners)	Can verify a user's RealMe login credentials.
T3	1	U1 (Dog Owners)	Can view their dog(s) registration data. Can alter some of the registration details, such as their pronouns, first/last names, email address, physical address, and name of their dog.
T4	0	U2 (Members of the Public)	Can access the user registration and Retrieve Lost Dog login pages, and the form for declaring a lost dog.

5) Entry Points:

ID	Name	Type	Description	Trust Levels
E7	User Registration	Added	Allows users to register with their personal information.	0
E8	Attempt Login	Added	Allows users to attempt a login with valid credentials.	0
E9	ACK Phone	Added	Sends information that the user pressed the # symbol and confirmed the login via 2FA.	0
E10	ACK Verify Identity	Added	Confirms with RealMe that the user is providing valid credentials.	2
E1	Registration Form	Modified	Altered to require a logged-in user	1
E2	Renew Form	Modified	Altered to require a logged-in user	1
E4	Lost Dog Form	Modified	Altered to require a logged-in user	1
E6	Terminate Registration Form	Modified	Altered to require a logged-in user	1

6) Exit Points:

ID	Name	Type	Description
X4	ACK Registration	Added	Acknowledges if the registration was successful or not.
X5	ACK Login	Added	Send data that acknowledges the login was successful or not.
X6	Make Call	Added	2FA Verification Step
X7	Verify Identity	Added	Uses the real me service to request the user to verify their identity.

7) Assumptions:

ID	**Type**	**Details**
S1	Modified	A user account registration is now used to access registrations.
S9	Added	The system has access to and can implement authentication with RealMe, the New Zealand government's official digital identification system.

8) Conclusion: Over all, the addition of a login system significantly increases the security of the system as it migrates and removes some of the vulnerabilities inherent in its old login-less design, such as the ability to spoof invoices, which can be used to steal money, or the ability to easily unregister someone's dog, forcing them to repay the registration fee.

but it also increases the system's complexity, both in the amount of effort it would take to create the system and in the amount of effort taken by a dog owner to do any action in the system.

B. Implement a support system that dog owners can contact if they experience issues with registration.

1) Reason: There are various things that could go wrong during the registration process. For example, an owner could lose access to their email address, or it could otherwise become compromised. The current model doesn't enable owners to update their email address, unless they terminate their dog's registration and register again, which costs money. Implementing a support system would give owners recourse to contact the council if anything goes wrong.

2) Assets:

ID	Type	Name	Description
A1	Modified	Personal details	Owner personal details may include two security questions and their answers, along with other possible identifying parameters, such as their date of birth.

3) Entry Points:

ID	Name	Type	Description	Trust Levels
E1	Dog Registration Form	Modified	Now includes security questions and a date of birth field.	0
E6	Support Call	Added	Owners can call the support line to speak to council staff about issues with their registration. As this is a public phone-line, anyone could potentially call in.	0

4) Exit Points:

ID	Name	Type	Description
X7	ACK Support	Added	Acknowledges if the support call and if any actions have taken place because of it.

5) Assumptions:

ID	**Type**	**Details**
S10	Added	The phone support number is publicly available, but the internal line can only be operated by council staff.

6) Dependencies:

ID	Name	Description
D8	Telephone System	Phone resources to handle calls.

7) Threats:

Type	Description	Mitigations	Severity	Mitigated?
Spoofing	Attackers could spoof the council staff on the phone that they are the dog owner and gain access	By training council staff so that detect fake owners. And by having more security questions or questions that would be harder to guess.	High	Yes
Denial of service	Attackers could flood the phone lines with a large number of fake calls.	By having a system that blacklist spam phone calls and by only accepting phone calls from nz phone numbers.	Medium	Yes
Information Disclosure	Attackers could intercept phone calls	By following industry standards for ensuring a secure phone call	Medium	Yes
Repudiation	A dog owner could get information changed on a phone call and latter claim they did not ask for it to be changed	By having a log of all phone calls to check against claims.	Low	Yes

8) Discussion: Having a support system brings many needed functional improvements and helps address some security vulnerabilities. However, it could also lead to additional security risks, as people might be able to spoof the system by phone. Furthermore, operating this system would incur significant costs, including the need for more council employees and the maintenance of the phone infrastructure.

C. Reinforcing against false terminations.

1) Reason: The current requirements for terminating a registration are knowing the dog's name, tag ID, and owner's email address. All three of these pieces of information could easily be obtained by, say, a malicious neighbour, or other member of the public with basic knowledge of the owner and access to the dog physically. This could be reinforced by both expanding the information required to terminate a dog's registration, such as by including the unique registration number itself, and by sending a confirmation email to the owner's email address before performing the termination.

2) Entry Points:

ID	Name	Type	Description	Trust Levels
E6	Terminate Registration Form	Modified	Now includes a field for the unique registration number.	0
E8	Confirm Termination From Link	Added	Page generated with unique token when a termination request is performed. Navigating to the page confirms and performs the termination.	0

3) Exit Points:

ID	Name	Type	Description
X7	Termination Email	Modified	The termination email no longer tells the owner that their registration has been terminated. Instead, it asks them to confirm they want to terminate their registration by clicking a provided link, and warns them that, if the request to terminate the registration is unexpected, they should contact the council.

4) Threats:

Type	Description	Mitigations	Severity	Mitigated?
Tampering	An attacker could modify the confirmation email link to redirect to a malicious webpage.	Send emails via TLS	Medium	Yes
Information Disclosure	An attacker could intercept the confirmation email, which now includes a link to terminate the dog's registration. This link is private, and shouldn't be visible to attackers.	Send emails via TLS	Medium	Yes
Elevation of Privilege	An attacker could guess the termination token through brute force, and terminate without being the owner.	Ensure the token generated upon a termination request is sufficiently complex. Instead of terminating upon navigating to the link, have a final confirmation on the page that requires owner details, such as their registration number.	Low	Yes

5) Discussion: The termination confirmation email still includes a link, which could be used in an attack to redirect the user to a fake website. That these emails exist and are being sent by the council also increases the risk of users receiving and falling for a false email, telling them (for example) that their registration will be cancelled unless they click a (malicious) link. A better solution to this problem is discussed above, where the user can only terminate their registration when logged in with appropriate email and password credentials.

D. Provide direct payment method

1) Reason: Paying by bank deposit is rather tedious, and owners would likely prefer to pay directly with their card via a payment service, like Stripe or Paypal. The bank deposit method also invites some security vulnerabilities, such as opening owners up to phishing attacks. Our assumptions are also that deposits and references are manually checked by council staff. This opens up two more risks: first, that a staff member overlooks a transaction, and second that an owner mistypes their reference number in the transaction. Adding an option to pay directly instead of bank deposit would thus improve the end-user experience, and mitigate some existing functional issues with the system.

2) Actors:

ID	Type	Name	Description
U6	Added	Automatic Payment System	A digital payment service provider for paying via card online.

3) Entry Points:

ID	Name	Type	Description	Trust Levels
E1	Registration Form	Modified	Now includes optional fields for paying directly, with an embedded external provider's form.	0
E2	Renew Form	Modified	Now includes optional fields for paying directly, with an embedded external provider's form.	0

4) Exit Points:

ID	Name	Type	Description
X8	External Payment	Added	Sends provided payment details to the external provider.

5) Dependencies:

ID	Name	Description
D9	Automatic Payment Provider	Service provider for automatic card payments, such as Stripe or Paypal.

6) Threats:

Type	Description	Mitigations	Severity	Mitigated?
Spoofing	Attackers could spoof the forms for registration and renewal, allowing them to capture the credit card details of the owner.	Purchase similar domains to the council website. Warn users on the website and via email about any known false domains. Educate users to check for the HTTPS lock icon in their browsers. Use an HTTPS form.	High	Yes
Spoofing	Dog owners could use stolen credit card details to pay for the registration.	Ensure the selected third-party payment service makes an effort to screen for known stolen credit card numbers.	Low	No
Repudiation	Owners could choose not to pay for their registration, then claim they had paid.	Ensure all attempts to pay through the third-party service, successful or not, are logged and available.	Low	Yes
Information Disclosure	An attacker could intercept the user's credit card details during form submission.	Use HTTPS to encrypt the payment information.	High	Yes
Information Disclosure	The third-party payment provider could be compromised by an attacker, exposing customer payment information.	Use a reputable provider that conforms to industry security best-practices.	High	Yes

7) Discussion: The external payment provider brings an obvious functional improvement to the system, and mitigates some existing security vulnerabilities. But it also opens up its own risks, and may not make the system more secure overall. External services carry their own risks, for one. PayPal experienced a substantial data breach at the end of 2022, compromising customer information for 35,000 of its users. Users inputting their credit card details into an online form also makes existing attacks, such as website spoofing (phishing) and man-in-the-middle attacks, much more potentially damaging.

III. Contributions

A. Whole Group

- Identification of actors
- Identification of assumptions
- Identification of constraints
- Identification of dependencies
- Identification of trust levels
- Identification of assets

B. Daniel Lowe

- Functional Change: Switching to a login-based authentication model
- Dog Data store Component
- log data store Component and arrows linked to it
- Register Dog Component and arrows linked to it
- Mail Service Component and arrows linked to it
- Dog Owner Component
- Dog Owner Component Component and arrows linked to it
- Tag manufacturing and sending system Component and arrows linked to it
- Manage Registration Component and arrows linked to it excluding sign in and ack sign in
- Wrote up the initials before meeting the constituents we use are mildly modified versions of these.
- Added Dependencies Description
- proof-reading

C. Isla Smyth

- Renew Registration Process and connected data-flows.
- Council Employee Actor and connected data-flows.
- Retrieve Lost Dog data flows
- Reinforcing against false termination
- Provide direct payment method
- Proof-reading

D. Chloe McLaren

- Animal Control and connected data-flows
- Members of public and connected data-flows
- Report Found Dog and connected data-flows
- Register and Renew Registration Components
- Threats and Mitigations
- Proof-reading, grammar and spell-checking

E. Campbell Shepherd

- Animal Control and connected data-flows
- Lost dog form and connected data flows
- Implement a support system improvement
- Threats and Mitigations
- Proof-reading, grammar and spell-checking

IV. Documents

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

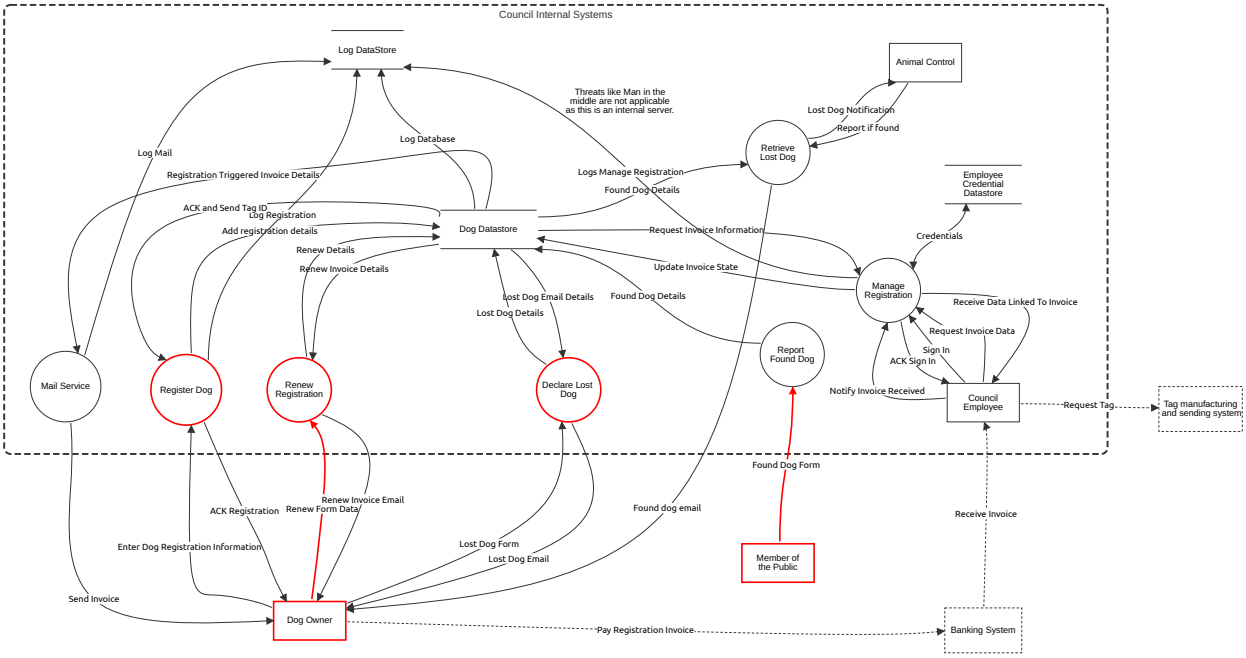
High level system description

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.

Council Dog Infrastructure Model (with login)

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

Executive Summary

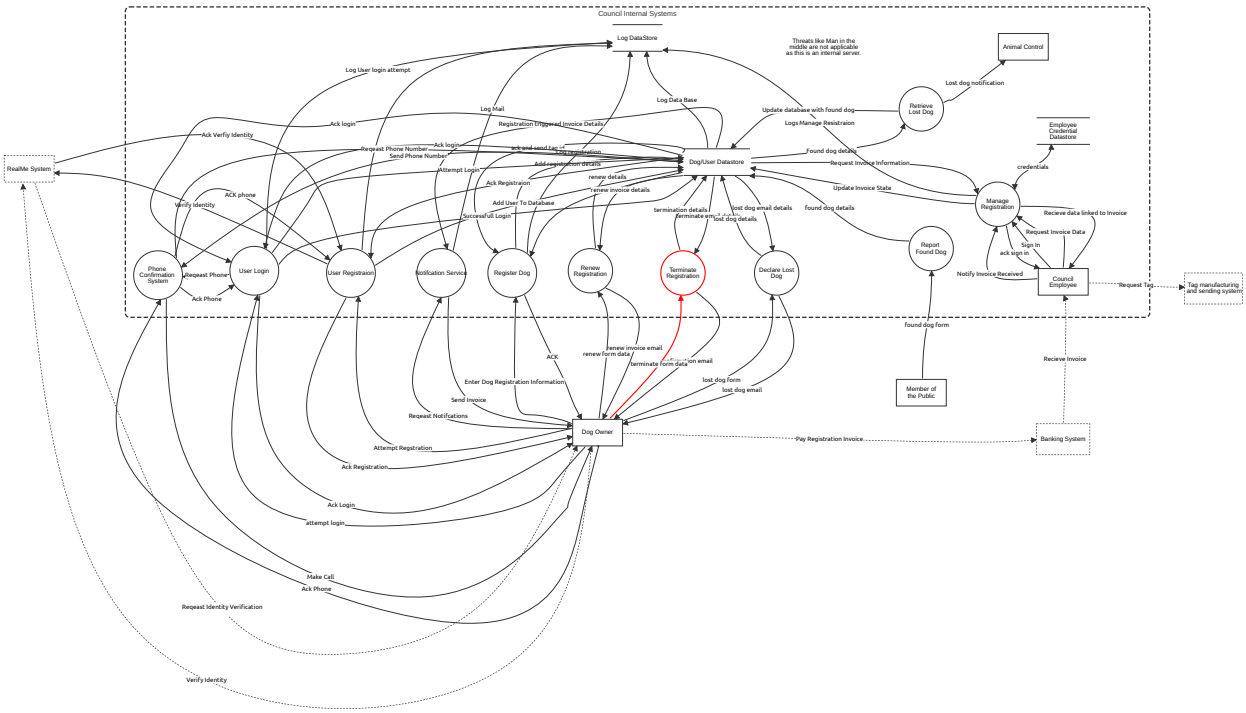
High level system description

Processes that require login do not have dataflows to the datastore and back to represent checking that the user is logged in because it would clutter the diagram well adding minimal information.

Summary

Total Threats	90
Total Mitigated	88
Not Mitigated	2
Open / High Priority	0
Open / Medium Priority	1
Open / Low Priority	1
Open / Unknown Priority	0

Login Diagram



Login 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

Register Dog (Process)

HTTPS web page endpoint(s) and api(s) that are used for dog registration.
(Requires the user to be logged in.)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
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
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/User Datastore (Store)

Stores information relating to dog and user 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 password with salt so that user information can only be received if you have the user name and password.
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.

terminate email details (Data Flow)

Contains details for personalising the termination confirmation email that were not obtained in the terminate process: the owner's full name and pronouns, and the registration ID.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

termination details (Data Flow)

Contains tag ID and flag for if a dog's registration has been terminated.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

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

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 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 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.

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.

confirmation email (Data Flow)

Personalised email addressed to the owner confirming that the dog of specified ID is no longer registered. Includes a link to the registration page.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
101	Data Tampering	Tampering	Medium	Mitigated		Data could be tampered with via a man-in-the-middle attack, altering the re-registration link to direct somewhere else.	Ensure the email is sent via TLS.
103	Data Interception	Information disclosure	Medium	Mitigated		The email could be intercepted, allowing an attacker to obtain the owner's pronouns, full name, and email address.	Ensure the email is sent via TLS.

terminate form data (Data Flow)

Form data sent for terminating a dog registration. Contains the owner's email address, tagID, and dog's name.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
99	Data Interception	Information disclosure	Medium	Mitigated		Form data could be intercepted, allowing an attacker to obtain the sender's email address.	Use HTTPS to encrypt the form data.
100	Flooding Attack	Denial of service	Medium	Open		Attackers could flood the termination form page with illegitimate 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.

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.
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.

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

Lost dog notification (Data Flow)

Notifies animal control about lost dogs and any information on them.
(Last address of dog, dog tag ID, dog breed, owner's address, etc)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
75	Information sent to more people	Information disclosure	Medium	Mitigated		Information sent to people in animal control who will not be dealing with the form.	Have the notification only sent to persons who will be collecting the dog

Number	Title	Type	Priority	Status	Score	Description	Mitigations
76	Flooded with fake notifications	Denial of service	Medium	Mitigated		If too many fake notifications are sent then animal control won't be able to accurately collect 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.
77	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.
112	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.

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

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 Resistraion (Data Flow)

Contains all actions taken while managing the registration.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Log Data Base (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

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

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

Recieve 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

Recieve 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

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

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Log User login attempt (Data Flow)

logs a users attempt at logging in

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Update database with found dog (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Ack Phone (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

ACK phone (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Ack login (Data Flow)

Ack if the login was successful or not.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

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.

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	Mitigated		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.

Reqeast Identity Verification (Data Flow) - *Out of Scope*

Reqeast a user identify their identity.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Verify Identity (Data Flow) - *Out of Scope*

the User Verifys Identity

Number	Title	Type	Priority	Status	Score	Description	Mitigations

attempt login (Data Flow)

Sends username and password to attempt to login

Number	Title	Type	Priority	Status	Score	Description	Mitigations
121	Man in the middle Tampering	Tampering	Medium	Mitigated		Someone could do a man-in-the middle attack 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.
122	Man in the middle, spying	Denial of service	Medium	Mitigated		Someone could spy on the information 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.

Ack Login (Data Flow)

Send data that acknowledges the login was successful or not.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
123	Man in the middle Tampering	Tampering	Medium	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.
124	Man in the middle, spying	Information disclosure	Medium	Mitigated		Someone could spy on the information 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.

Ack Phone (Data Flow)

Sends infomation that the user pressed the # sysmbol and confirmed the login

Number	Title	Type	Priority	Status	Score	Description	Mitigations
133	Man in the middle Tampering	Tampering	Low	Mitigated		Someone could do a man-in-the middle attack and manipulate the data while it is in transit.	Use secure protocols to encypt the data in transit.
134	Man in the middle, spying	Information disclosure	Medium	Mitigated		Someone could do a man-in-the middle attack and view the data while it is in transit.	Use secure protocols to encypt the data in transit.

Make Call (Data Flow)

The phone call that is make to the person

Number	Title	Type	Priority	Status	Score	Description	Mitigations
131	Man in the middle Tampering	Tampering	Low	Mitigated		Someone could do a man-in-the middle attack and view and manipulate the data while it is in transit.	Use secure protocols to encypt the data in transit.
132	Man in the middle, spying	Information disclosure	Low	Mitigated		Someone could do a man-in-the middle attack and view the data while it is in transit.	Use secure protocols to encypt the data in transit.

Ack Verfiy Identity (Data Flow)

Ack knowlages if the person is who they say they are

Number	Title	Type	Priority	Status	Score	Description	Mitigations
147	man-in-the middle Tampering	Tampering	Medium	Mitigated		Someone could do a man-in-the middle attack 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.
148	man-in-the middle Spying	Information disclosure	Medium	Mitigated		Someone could do a man-in-the middle attack and Spy on 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.

Verify Identity (Data Flow)

Uses the real me service to request the user to verify their identity.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
145	man-in-the middle Tampering	Tampering	Medium	Mitigated		Someone could do a man-in-the middle attack 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.
146	man-in-the middle spying	Information disclosure	Medium	Mitigated		Someone could do a man-in-the middle attack and Spy on 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.

ACK (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

Attempt Regstration (Data Flow)

Contains the users

Number	Title	Type	Priority	Status	Score	Description	Mitigations
140	Tampering	Tampering	Medium	Mitigated		Someone could do a man-in-the middle attack 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.
141	Information Disclosure	Information disclosure	Medium	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.

Ack Registration (Data Flow)

Acknowledges if the registration was successful or not.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
135	Man in the middle Tampering	Tampering	Medium	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.
136	Man in the middle, spying	Information disclosure	Medium	Mitigated		Someone could spy on the information 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.

Attempt Login (Data Flow)

The users username and password are sent(hashed) and checked agenst the data base to see if there is a match

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

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Ack Registraion (Data Flow)

Ack if the registration was successful or not.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Add User To Database (Data Flow)

Adds a user to the database with the given details

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Ack login (Data Flow)

Sends if the login was successfull or not for the user

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Send Phone Number (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Reqeast Phone (Data Flow)

Require a phone call be sent out to the given user.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Reqeast Phone Number (Data Flow)

Require a phone number for a given user

Number	Title	Type	Priority	Status	Score	Description	Mitigations

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

Successfull Login (Data Flow)

Tell the system the login was successful (after phone).

Number	Title	Type	Priority	Status	Score	Description	Mitigations

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	Data manipulation	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	Information 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.

Reqeast Notifcations (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Send Invoice (Data Flow)

Notifies the user of the invoice.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
149	Data manipulation	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.
150	Informatoin disclosure	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.

Renew Registration (Process)

HTTPS webpage endpoint(s) for renewing a dog's registration.
(Requires the user to be logged in.)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
86	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
87	False Information	Spoofing	Low	Mitigated		Users could provide incorrect renewal details, such as an invalid address.	Validate addresses syntactically and through a location API.
88	Claim against renewal	Repudiation	Low	Mitigated		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		See renew form data	
90	Data Tampering	Tampering	Medium	Mitigated		See renew form data	
91	Flooding Attack	Denial of service	Medium	Mitigated		See renew form data	
142	Fake Renew	Tampering	Medium	Mitigated		Renew someone else's dog without their consent or knowledge.	Requires you to be logged in, which requires two-factor authentication.

Terminate Registration (Process)

HTTPS webpage endpoint(s) for terminating a dog's registration.
(Requires the user to be logged in.)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
94	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
95	False Information	Spoofing	Low	Open		Users could provide incorrect termination details, such as an invalid address.	Validate addresses syntactically and through a location API.
96	Claim against termination	Repudiation	Low	Mitigated		Owners could claim they hadn't performed a registration termination when they had.	- Log all termination actions to the system. Include relevant information about the request, i.e., IP address, time/date
97	Data Interception	Information disclosure	Medium	Mitigated		See terminate form data	
98	Flooding Attack	Denial of service	Medium	Mitigated		See terminate form data	

Number	Title	Type	Priority	Status	Score	Description	Mitigations
143	Fake Termnate	Tampering	High	Mitigated		Termnate someone else's dog without their consent or knowledge, forcing them to repay the registration fee for their dog.	It requires you to be logged in, which requires two-factor authentication.

Declare Lost Dog (Process)

HTTPS webpage endpoint(s) for declaring a dog as lost.
(Requires the user to be logged in.)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
67	Fake dog owner	Spoofing	Medium	Mitigated		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.
144	New STRIDE threat	Spoofing	Medium	Mitigated		Declare a dog is lost that is not lost, wasting animal control time.	You need to be logged in to declare your dog lost, and any dogs declared lost in this way are logged so if it is found that they are not lost then they can know who lied.

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	Mitigated		Member of the public inputs incorrect dog tag or address (intentionally or unintentionally)	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 Misuse of Personal Data	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 Misuse of tag paid system	Tampering	Medium	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

Notifcation Service (Process)

Used to notify user of changes invoices.
(Requires the user to be logged in.)

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 notification sender and keep a stack of all the emails that still need to be sent.
115	Fake Invoice	Spoofing	Medium	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 are sent using the internal system so they would need access to the system to do this.

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

User Registraion (Process)

Registers someone with the provided name and RealMe account and password.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
137	Flood Endpoint	Denial of service	Low	Mitigated		Someone could flood the endpoint with fake login attempts to force the endpoint down.	Use IP blocking to prevent one address from being repeatedly used.
138	Pretend to be someone else.	Spoofing	Medium	Mitigated		Someone could possibly put in fake information to their registration, so if an investigation is needed for a mistreatment of their dogs while they are not at home, then they can blame someone else.	Use RealMe to verify a person's details and request they verify their phone number by calling it.
139	Phishing Attacks	Spoofing	Medium	Mitigated		Fake registration pages designed to steal personal information, including usernames, passwords, and financial details.	- Prioritise shorter URLs - Purchase and redirect from similar domains

User Login (Process)

Used to log users in

Number	Title	Type	Priority	Status	Score	Description	Mitigations
125	Wbsite spoofing	Spoofing	Low	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
126	Fake login	Spoofing	Medium	Mitigated		Someone could log in as someone else.	All passwords are required to be at least 8 characters long and contain a number, letter, and special charter. Use a CAPTCHA to prevent them from automating it. Reqiure two factor authencation of the phone call From M1036 Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. (Use 3 attempts and 10 minites before the next allowed attempt from the IP address or for that specific account.)
127	Flood Endpoint	Denial of service	Medium	Mitigated		Some one could flood the endpoint with fake login attempts to force the end point down.	Use IP blocking to prevent one address from being repetedly used.
128	Flood User acount.	Denial of service	Medium	Mitigated		Someone could repeatly fake attempting to login in to an account to trick the system into makeing that account not useable.	Use a CAPTCHA to prevent them from automating it and block IP addresses that repeatedly attempt to login to the same account.

Phone Confirmation System (Process)

rings someones phone and reqires them to press the # for them to login to there account.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
125	Website Spoofing	Spoofing	Low	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
126	Fake login	Spoofing	Medium	Mitigated		Someone could log in as someone else.	All passwords are required to be at least 8 characters long and contain a number, letter, and special charter. Use a CAPTCHA to prevent them from automating it. From M1036 Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. (Use 3 attempts and 10 minites before the next allowed attempt from the IP address or for that specific account.)
127	Flood Endpoint	Denial of service	Medium	Mitigated		Some one could flood the endpoint with fake login attempts to force the end point down.	Use IP blocking to prevent one address from being repetedly used.
128	Flood User acount.	Denial of service	Medium	Mitigated		Someone could repeatly fake attempting to login in to an account to trick the system into makeing that account not useable.	Use a CAPTCHA to prevent them from automating it and block IP addresses that repeatedly attempt to login to the same account.

RealMe System (Actor) - *Out of Scope*

The NZ digital ID service.

Number	Title	Type	Priority	Status	Score	Description	Mitigations