Assignment 2
Council Dog Registration System
STRIDE Report

Group 2

Daniel Cha
James Suddaby
Kane Xie
Mohammad Munem

9th August 2024

1 Actors

ID	Name	Description
A1	Dog Owner	A person living in the jurisdiction of the Council who owns one or more dogs.
A2	Member of the public	Anonymous user who may or may not own a dog.

2 External Dependencies and 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	The connection between the web server and the database server will be over a private, secure and end-to-end encrypted network. e.g., The dataflow from register a dog process to dog details datastore is secure.
C5	The Council Dog web application will run on a Linux server running Apache. This server will be hardened per the council's server hardening standard. This includes the installation of the latest operating system and application security patches.
C6	The database server for storing user details will be MySQL and it will run on a Linux server. This server will be hardened per the council's server hardening standard. This will include the installation of the latest operating system and application security patches.
C7	The web server is behind a firewall and the only communication available is TLS.
C8	The web application must be available 24/7.
C9	The web application uses an external API process to send emails. The external API process has its own security system. Due diligence is done to make sure of its integrity.
C10	The council uses an external service or process to pick up dogs. This external process has its own security system. Due diligence is done to make sure of its integrity.
C11	A dog is only registered into the system once the dog registration payment is received from the dog owner.

C12	The external email API has its own security and is outside the control of the web app but .
C13	Dog pickup services require information on the dog's name, breed, tag ID, and physical address to pick up a dog.
C14	The web app is not providing any payment method. It is up to the user to choose their bank and the bank's payment method to transfer money.

3 Trust Levels

ID	Name	Description
T1	Anonymous user	A user who accesses the web application but has no dogs associated with their email.
T2	Dog owner	A user who accesses the website and has dogs associated with their email.
T3	Database Admin	The database admin (A member of the council) has the read and write privileges to database servers.
T4	Website Admin	A member of the council responsible for the maintenance and configuration of the website.
T5	Email process	API service that provides emailing capabilities
T6	Banking process	Bank services that users use to pay registration fees
T7	Dog pickup service	Dog services responsible for picking up found dogs
T8	Dog tag manufacturing process	Manufacturer that makes and sends dog tags to owners

T9	Database Read User	The database user account used to access the database with only read privileges.
T10	Database Read/Write User	The database user account used to access the database with read and write privileges.
T11	Web server User Process	The user account that the web server authenticates itself to the database and executes the code.

4 Entry Points

ID	Name	Description	Trust Levels
EN1	HTTPS Port	The dog registration web app will only be accessible via TLS. All pages within the website are layered on this entry point.	(1) Anonymous web user (2) Dog Owner (3) Website admin
EN1.1	Home page	Landing page for website. Other pages are accessible from here.	(1) Anonymous web user (2) Dog Owner (3) Website admin
EN1.2	Dog registration page	Webpage for registering a dog.	(1) Anonymous web user (2) Dog Owner (3) Website admin
EN1.2.1	Dog registration function	The registration function takes in dog and dog owner details to register a dog in the database.	(2) Dog Owner (3) Website admin
EN1.3	Dog registration renewal page	Webpage for renewing a dog's registration.	(1) Anonymous web user (2) Dog Owner (3) Website admin

EN1.3.1	Dog registration renewal function	Takes in dog and dog owner details and compares it with the database.	(2) Dog Owner (3) Website admin
EN1.4	Dog registration termination page	Webpage for terminating a dog's registration.	(1) Anonymous web user (2) Dog Owner (3) Website admin
EN1.4.1	Dog registration termination function	Takes in dog details and owner's email address and compares it with the database.	(2) Dog Owner (3) Website admin
EN1.5	Declare lost dog page	Webpage for reporting a lost dog.	(1) Anonymous web user (2) Dog Owner (3) Website admin
EN1.5.1	Declare lost dog function	Takes in the dog's name and dog owner's email address and compares it with the database.	(2) Dog Owner (3) Website admin
EN1.6	Report found dog page	Webpage for reporting a found dog.	(1) Anonymous web user (2) Dog Owner (3) Website admin
EN1.6.1	Report found dog function	Takes in the dog tag ID and pickup address and compares it with the database.	(1) Anonymous web user (2) Dog Owner (3) Website admin
EN2	Bank payment service	Takes in payment information to check whether fees have been paid	(3) Website admin (6) Banking Process
EN2.1	Registration payment check	Takes in payment information to check whether registration fees have been paid	(3) Website admin (6) Banking Process
EN2.2	Renewal payment check	Takes in payment information to check whether renewal fees have been paid	(3) Website admin (6) Banking Process

5 Exit Points

ID	Name	Description	Trust Levels
EX1	HTTPS port	Website pages are served to users via HTTP.	(1) Anonymous web user (2) Dog Owner (3) Website admin
EX1.1	Dog registration confirmation page	A confirmation message including the registration number and expiry date.	(1) Anonymous web user (2) Dog Owner (3) Website admin
EX1.2	Lost dog confirmation page	A page acknowledging the dog's "lost" status, including the latest dog tag ID.	(2) Dog Owner (3) Website admin
EX2	Email	User information is sent via email.	(2) Dog Owner (3) Website admin (4) Database admin (5) Email process
EX2.1	Dog registration confirmation email	An email with an invoice for registering the dog.	(2) Dog Owner (3) Website admin (5) Email process
EX2.2	Dog registration renewal confirmation email	An email containing an invoice.	(2) Dog Owner (3) Website admin (5) Email process
EX2.3	Dog registration termination confirmation email	An email containing the termination confirmation message.	(2) Dog Owner (3) Website admin (5) Email process
EX2.4	Lost dog confirmation email	An email confirming that the dog has been reported as lost.	(2) Dog Owner (3) Website admin (5) Email process
EX2.5	Found dog email	An email notifying the owner that their dog has been found.	(2) Dog Owner (3) Website admin (5) Email process

EX3	Dog pickup service	Communications with the dog pick up services on the dog to pick up.	(3) Website admin (7) Dog Pickup service
EX4	Tag manufacture and sending service	Information on the dog tag ID and physical address is sent to the service.	(3) Website admin (8) Dog tag manufacturing service
EX4.1	Registration tag manufacture	Making a new dog tag for a newly registered dog.	(8) Dog tag manufacturing service
EX4.2	Renewed tag manufacture	Making a new dog tag for a renewed dog registration.	(8) Dog tag manufacturing service

6 Assets

ID	Name	Description	Trust Levels
AS1	**Web Application Users**	**Assets relating to Dog owner and Dog.**	
AS1.1	Banking details of the dog owner	The banking credentials i.e. account no. and account name that a dog owner used to pay for the tag.	(2) Dog Owner (3) Website admin (4) Database admin (9) Database Read User (10) Database Read/ Write User
AS1.2	Personal data of the dog owner	The web application will store personal information relating to the dog owner.	(2) Dog Owner (3) Website admin (4) Database admin (9) Database Read User (10) Database Read/ Write User
AS1.3	Dog details	The web application will store information relating to the dog's name, breed, status and tag ID.	(2) Dog Owner (3) Website admin (4) Database admin

			(9) Database Read User (10) Database Read/ Write User
AS2	**System**	**Assets relating to the underlying system.**	
AS2.1	Availability of Web Application	The web application is available 24/7 and can be accessed by all the members of the public and dog owners.	(3) Website admin (4) Database admin
AS2.2	Ability to Execute Code as a Web server User	This is the ability to execute source code on the web server as a web server user.	(3) Website admin (4) Web server User Process
AS2.3	Ability to fetch data as a Database Read User	This is the ability to fetch data from the database as a Database Read User.	(5) Database Admin (8) Database Read User (9) Database Read/Write User
AS2.4	Ability to send and fetch data as a Database Read/Write User	The ability to send or fetch any data from the database as Database Read/Write User.	(5) Database Admin (9) Database Read/Write User
AS3	**Web Application**	**Assets relating to the web application.**	
AS3.1	Online/ Offline Session	This is the online session of a user on the web application. This user could be a Dog Owner or a member of the public.	(3) Website Admin
AS3.2	Access to the Database Server	Access to the database will allow administration access to the database allowing full access to the database.	(5) Database Server Admin
AS3.3	Ability to Create dog tags	The ability to create dog tags would allow an individual to create new dog tags on the system.	(3) Website Admin

AS3.4	Access to the banking process	Allows access to the banking data handling system.	(3) Website Admin (5) Database Admin
AS3.5	Access to the external email API	Allows access to the email API. Ability to send and receive email.	(3) Website Admin (5) Database Admin
AS3.6	Access to the dog tag manufacturer	Allows access to the manufacturer of the dog tags. Ability to manufacture dog tags	(3) Website Admin (5) Database Admin
AS3.7	Access to the dog pick up service	Allows access to the dog pick up service. Ability to ask for a dog pick up.	(3) Website Admin (5) Database Admin

7 Potential Improvements

A threat analysis of the improved system is given in Section 11.

ID	Improvement name	Related functional aspect	Proposed change
P1	Limit access	1.1 Dog registration & 1.2 Declaring a lost dog	Apply Principle of Least Privilege and restrict access to certain functions based on user authentication status. **Dog owners A1** can: ● Log in to the application ○ Register a dog ○ Renew a dog registration ○ Terminate a dog registration ○ Declare their dogs as lost ● Report a dog as found **Members of the public A2** can: ● Report a dog as found
P2	Registration and login system	1.1 Dog registration & 1.2 Declaring a lost dog	A user can register themselves as a **dog owner A1** and gain access to more functionality than a **member of the public A2** would have. After registration they can login to the system with their information. Below are the details required for registration and login: Registration ● Email ● Password ● First name, last name, pronoun ● Physical address

			Login • Email • Password
P3	Email address verification upon registration	1.1 Dog registration & 1.2 Declaring a lost dog	When registering a new account, **dog owners A1** will need to verify their email address by clicking a confirmation link sent to their email. If the email address is not verified, the **dog owner A1** account will not be activated.
P4	Two factor authentication for logging in	1.1 Dog registration & 1.2 Declaring a lost dog	When logging into the website from a new IP or after 1 week, the **dog owner A1** must enter a code sent to their email address along with their email address and password.
P5	Additional information when reporting a found dog	1.3 Reporting a found dog	When reporting a found dog, the user has to input their email address, photo of the dog with the dog tag ID visible, dog tag ID, and the physical address where the dog is currently located.
P6	Flag multiple found dog reports coming from the same email	1.3 Reporting a found dog	If multiple reports of a found dog come from the same email within a small amount of time, it should be flagged.
P7	Email confirmation for reporting found dogs	1.3 Reporting a found dog	When a found dog report is submitted, the reporter receives an email with a confirmation link that they must click to validate their report.
P8	Confirm Dog is lost	1.3 Reporting a found dog	When a dog is reported as found, despite not being declared as 'lost', the **dog owner A1** receives an email notification informing them that someone is attempting to report their dog as found. They will be able to confirm whether the dog was ever lost or not.

8 Discussion

After conducting the threat model analysis for the council dog app, we have identified several areas of improvement that can increase the security of the application by providing some mitigations to open threats.

8.1 Improvements regarding 1.1 Dog registration and 1.2 Declaring a lost dog

In the initial design of the application we identified fraudulent reporting threats in a number of the processes whereby a malicious actor could use the dog ID and dog owners email to change the registration status of the dog *(Terminate a registration process - #2, Renew dog registration process - #130)* or declare a dog lost lost *(Declare lost dog process - #85)*. In response to unmitigated threats in these processes, we have proposed some improvements to limit access and mitigate threats such as spoofing and repudiation.

We identified that in the original design there were no limitations to who could interact with what functions. This makes it very easy for bad actors to access and interact with our system. The improvement **P1** involves applying the Principle of Least Privilege to restrict access to specific functions based on user authentication status. In the original system, **members of the public - A2** can perform certain actions that should be restricted to **dog owners - A1**, such as 1.1.3 terminating a dog's registration and 1.3 declaring a dog as lost. This unrestricted access presents threats of fraudulent activities where a malicious actor could exploit these capabilities. We recommend that access to the 1.1 dog registration and 1.3 lost dog reporting features should be limited to just **dog owners - A1**. This improvement reduces the threat of unauthorised reporting and malicious alterations to dog statuses.

We recommend implementing improvement **P2**, a registration/login system, to reduce the likelihood of bad actors performing actions that could lead to repudiation. The improved system requires users to register with detailed personal information including their email address, password, full name, pronouns, and physical address. After registration, **dog owners - A1** can access a broader range of functionalities. This improvement requires the user to use a sufficiently strong password: 8 chars long, upper/lower case, numbers and a special character. The registration process not only verifies the identity of users but also segregates the privileges granted to registered **dog owners - A1** versus **members of the public - A2**, thus enhancing overall system integrity and security.

We recommend the implementation of **P3** registration verification. The dog owner must verify their registration to the system by clicking on a confirmation link sent to their email address. This step is crucial in preventing the creation of fraudulent accounts and ensuring that all user actions are reliably linked to a verified email address, thus mitigating threats associated with unverified account activities. This also ensures that users who sign up have access to the email they are registering with, providing additional mitigation against repudiation threats.

While logging in to the application with strong credentials lowers the risk of spoofing attacks, it does not eliminate it. We recommend that **P4** two factor authentication be implemented to ensure that the user entering the credentials is the owner of those credentials. Log in attempts will require two-factor authentication if the log in occurs on a new IP or if it is more than a week since their most recent log in. The two-factor authentication works by requiring the users to enter a code sent to their email address. This helps prevent unauthorised access and ensures that the person attempting to log in is indeed the legitimate account holder.

8.2 Improvements regarding 1.3 Reporting a found dog

Another area of the system that would benefit from improvements is the found dog reporting system. In response to the identified threats within the original system, we have proposed several improvements aimed at enhancing the overall security and reliability of the process. These measures are designed to mitigate various threats such as spoofing, repudiation and denial of service.

The first improvement **P5** involves the introduction of mandatory fields for reporting a found dog. Reporters are now required to provide their email address, a photo of the dog showing the dog tag ID, the dog tag ID number, and the physical address of the dog. This change addresses critical gaps in the original system, which did not require an email address or photo evidence, potentially allowing for false reports with no accountability or traceability. By requiring this additional information **P6**, we address and mitigate threats **#80** and **#83** in the report a found dog process. Without these improvements, the system remains vulnerable to spoofed reports with no means to verify the authenticity or trace the origin, potentially leading to misuse of the reporting process and wasted resources on false leads. To prevent potential denial of service attacks manifested through an overwhelming number of false reports, we recommend a system that flags multiple reports from the same email address within a short period. This improvement ensures that unusual patterns of reporting are scrutinised and managed proactively. If unimplemented, attackers could flood the system with numerous false reports, overwhelming it and obstructing the processing of genuine reports. With this improvement, the system can better identify potential attackers, enhancing the system's ability to discern trustworthy reports from malicious ones.

Another improvement is the introduction of an email confirmation step for report submissions **P7**. Reporters must verify their report via a confirmation link sent to the entered email address. This not only deters false reports by adding an additional layer of user verification but also assists in authenticating the reporter's identity, significantly reducing the chances of spoofing. The email link acts as a digital footprint, linking the report to a specific email address and thereby providing a traceable path in case of disputes or investigations. Finally, we are proposing a direct verification process with **dog owners - A1** when their dog is reported as found without a prior 'lost' status **P8**. This alerts owners to potential misuse of their dog's tag ID and involves them directly in the verification process. By requiring owner confirmation on whether the dog was actually lost, we address spoofing threats where individuals might falsely report a dog as found. Without this confirmation process, there is a

risk that dogs not actually lost could be reported as such, causing unnecessary distress to owners and potentially leading to false claims. This measure ensures that only legitimate cases of lost dogs are pursued, preserving focus on genuine reports.

9 Contributions

All sections were discussed as a team.

Name:	Sections contributed	Contribution percentage (%)
James Suddaby	Original 1.1.3 stride diagram and threats. 4,5,7,8	25%
Daniel Cha	1, 2, 3, 4, 5, 7, 8.1, 8.2, Original system diagram, STRIDE threats for 1.3	25%
Kane Xie	1, 2, 3, 4, 5, 7, Original 1.1.1 and 1.1.2 STRIDE diagrams, new diagram after improvements	25%
Mohammad Munem	1, 2, 3, 4, 6, STRIDE threats for 1.3	25%

10 Threat Dragon Report

Council Dog Registration SystemSTRIDE Report

Owner: Fabian Gilson
Reviewer: Morgan English
Contributors: James Suddaby, Kane Xie, Daniel Cha, Mohammad Munem
Date Generated: Fri Aug 16 2024

Executive Summary

High level system description

The assignment of SENG406 is about a Dog register web app. A web-based application designed to register dogs in order to get their identification tags, as well as the management and traceability of dogs. Owners can register their dogs, and receive or renew their unique tags delivered by the Council. Dogs can be declared lost or found, and owners can terminate a registration before its expiration date.

The app, as we define it, exposes the following (simplified) features:
* individuals can register their dog to the app and order dog tags.
* individuals can renew their dog tags and get the new dog tags.
* the council delivers the dogs tags to the user.
* member of the public can report potential lost dogs.
* the council picks up the lost dog and notifies the dog owner.

End-user app
* Does not store private details, i.e. contact details, address, and bank / PayPal account (stored in private database)
* Registers a dog
* Renew a registration
* Terminate a registration
* Declare a lost dog
* Report of found dog

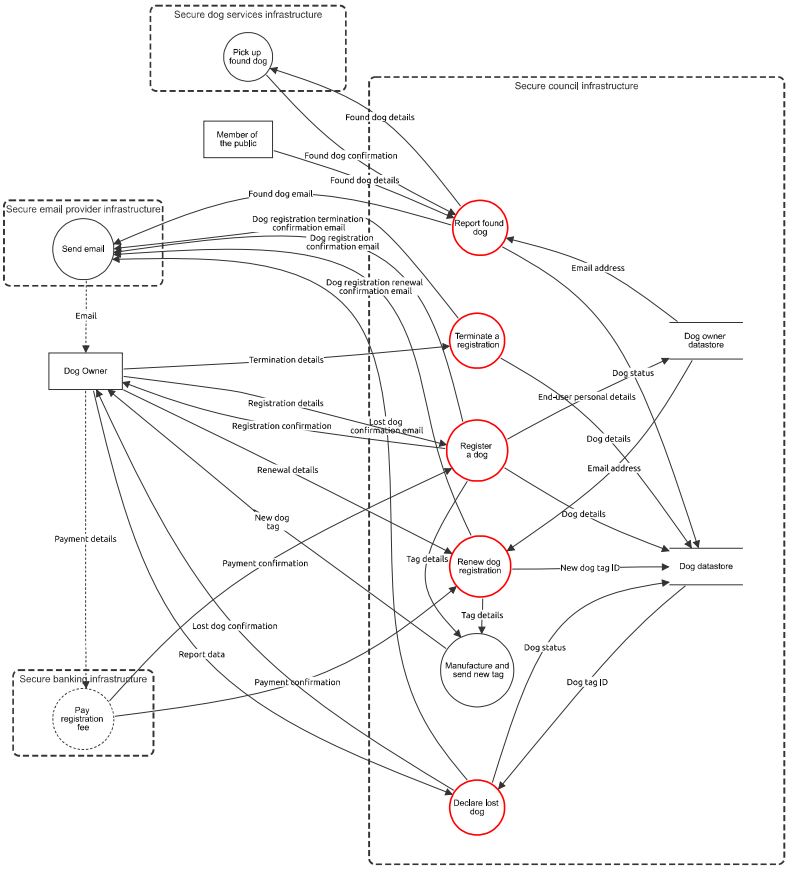
Trust levels (privileges):
1 Anonymous user
2 Dog owner
3 Database Administrator
4 Website Administrator
5 Email process
6 Banking process
7 Dog pickup service
8 Dog tag manufacturing process
9 Database Read User
10 Database Read/Write User
11 Web server User Process

Summary

Total Threats	141
Total Mitigated	135
Not Mitigated	6
Open / High Priority	0
Open / Medium Priority	6
Open / Low Priority	0
Open / Unknown Priority	0

11 Original system

STRIDE diagram for the original system



11 Original system

Register a dog (Process)

Action to register a dog.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
64	Fake personal information	Spoofing	Medium	Open		A dog owner could use fake personal information, such as name and physical address, when registering a dog. They would then be able to deny affiliation with the dog.	* Track payment details for registrations
66	Flooding of requests from the same IP	Denial of service	Medium	Mitigated		User trying to register large numbers of dogs at the same time.	* Add a cooldown time for the same IP to register another dog * Implement rate limiting to restrict the number of requests a single IP address can make * Use CAPTCHA on the registration form to prevent automated bots
132	User claims to have made payment	Repudiation	Medium	Mitigated		The user falsely claims they have paid the registration fee (denies not paying).	* Keep a copy of bank receipts, including the registration number reference and timestamps * Use digital signatures for payment receipts and invoices * Integrate an automated payment gateway that verifies the payments in real-time
140	Malformed data	Tampering	Medium	Mitigated		Same as #86	Same as #86
144	Adversary in the middle changes the registration details	Tampering	Medium	Mitigated		An adversary-in-the-middle intercepts the registration and modifies its content (e.g., email address and physical address)	* Use secure connection, http-only and secure cookie with unique session id * Sign (hash) content with user's private key

Dog Owner (Actor)

A person living in the jurisdiction of the Council who owns one or more dogs.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Dog details (Data Flow)

Includes:
* Dog name
* Dog breed
* Dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations

New dog tag ID (Data Flow)

Includes:
  * Old tag ID
  * Dogs new tag ID
to replace with the old one

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Tag details (Data Flow)

Includes:
  * Dog owners postal address
  * Renewed dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations

End-user personal details (Data Flow)

Includes:
  * Pronoun
  * First and last name
  * Email address
  * Physical address

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Tag details (Data Flow)

Includes:
  * Dog owners postal address
  * Unique dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Dog details (Data Flow)

Includes:
- Details of the dog to delete:
  * Dogs Tag ID
  * Dog name
  * Dog breed

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Payment confirmation (Data Flow)

Includes:
- Banking details
  * Account Name

* Account Number
* Registration Number

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Registration confirmation (Data Flow)

Includes:
* owner email
*Unique registration number,
*Expiry date for registration

Number	Title	Type	Priority	Status	Score	Description	Mitigations
101	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
109	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Report data (Data Flow)

Includes:
* Email address used to register the dog
* Dog's name

Number	Title	Type	Priority	Status	Score	Description	Mitigations
91	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
105	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Lost dog confirmation (Data Flow)

Includes:
* Dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations
98	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
106	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Dog tag ID (Data Flow)

Includes:
* Dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Email address (Data Flow)

Includes:
* Dog owner's email address

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Dog status (Data Flow)

Includes:
* Dogs new Status : FOUND
* Dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Found dog email (Data Flow)

Includes:
* Dog owner's email address
* Dog tag ID
* Dog found message

Number	Title	Type	Priority	Status	Score	Description	Mitigations
112	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
113	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Dog registration termination confirmation email (Data Flow)

Includes:
* Dog owner's email address
* Termination confirmation message
* dog's registration link

Number	Title	Type	Priority	Status	Score	Description	Mitigations
121	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103
122	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71

Dog registration confirmation email (Data Flow)

Includes:
* Invoice PDF (with amount and registration number)
* Email address
* Email content

Number	Title	Type	Priority	Status	Score	Description	Mitigations
115	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71

Number	Title	Type	Priority	Status	Score	Description	Mitigations
116	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Dog registration renewal confirmation email (Data Flow)

Includes:
* Invoice PDF
* Email address
* Email content

Number	Title	Type	Priority	Status	Score	Description	Mitigations
117	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103
118	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71

Lost dog confirmation email (Data Flow)

Includes:
* Dog tag ID
* Updated dog status

Number	Title	Type	Priority	Status	Score	Description	Mitigations
119	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
120	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Dog status (Data Flow)

Includes:
* Email address used to register the dog
* Dog's name
* Dog's new status: LOST

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Email address (Data Flow)

Includes:
* Dog owners email address

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Termination details (Data Flow)

Includes:
* Email address
* Dog tag ID
* Dog name

Number	Title	Type	Priority	Status	Score	Description	Mitigations
63	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
110	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Renewal details (Data Flow)

Includes:
* Dog tag ID
* Delivery address

Number	Title	Type	Priority	Status	Score	Description	Mitigations
100	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
108	Insecure connection	Tampering	Medium	Mitigated		Same as #103, an attacker could change the address to steal a dog's tag.	Same as #103

New dog tag (Data Flow)

Includes:
* Dog owners postal address
* Renewed dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations
99	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
107	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Found dog confirmation (Data Flow)

Includes:
* Dog tag ID
* Found location

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Registration details (Data Flow)

Includes:
- Personal details:
  * Pronoun
  * First and last name
  * Email address
  * Physical address

- Dog details:
  * Dog name
  * Dog breed

Number	Title	Type	Priority	Status	Score	Description	Mitigations
71	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		An adversary-in-the-middle intercepts the data and reads sensitive information.	* Protect data using TLS * Isolate the communication channels used for transmitting sensitive data * Implement secure communication channels
103	Insecure connection	Tampering	Medium	Mitigated		Data can be tampered by an adversary in the middle where the information can be modified.	* Use TLS to encrypt the data in transit * Implement hashing to create a checksum of the data before transmission and verify it upon receipt * Enforce HTTPS by implementing HSTS, which instructs browsers to only interact with the server over a secure HTTPS connection

Found dog details (Data Flow)

Includes:
  * Dog name
  * Dog breed
  * Dog tag ID
  * Pick up location address

Number	Title	Type	Priority	Status	Score	Description	Mitigations
123	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
124	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Found dog details (Data Flow)

Includes:
  * Dog tag ID
  * Physical address

Number	Title	Type	Priority	Status	Score	Description	Mitigations
79	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
147	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Payment confirmation (Data Flow)

Includes:
- Banking details
  * Account Name
  * Account Number
  * Registration Number

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Email (Data Flow) - *Out of Scope*

Email containing the relevant information.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Payment details (Data Flow) - *Out of Scope*

Includes:
- Banking details
  * Account Name
  * Account Number
  * Registration Number

Number	Title	Type	Priority	Status	Score	Description	Mitigations
102	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
104	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Dog datastore (Store)

This database contains the details of the dogs, including their name, breed, status, registration number, expiry date, tag ID, and owner.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	Unauthorised modification of dog data	Tampering	Medium	Mitigated		An attacker might gain unauthorised access and alter the information of the dog (e.g., name, lost status, owner, dog tag ID).	* Utilise hashing and checksum mechanisms to detect and prevent unauthorised changes to data * Implement role based access controls to restrict database write permissions to authorised personnel only * Regular audits and integrity checks on the database to identify any unauthorised changes
6	Dog datastore unwanted access	Information disclosure	Medium	Mitigated		Sensitive information might be exposed to unauthorised individuals.	* Datastore credentials are securely stored on password vaults with limited set of users having access (apply least privilege principle). * Datastore credentials are injected into connecting software from secured variables or files (apply least privilege principle).
7	Disputed data changes	Repudiation	Medium	Mitigated		An attacker or insider could dispute or deny making changes to records within the datastore, leading to challenges in auditing and accountability.	* Maintain detailed, tamper-evident logs of all actions performed on the datastore, including timestamps, user IDs, and specific changes * Use cryptographic signatures on logs * Restrict access to the datastore and its logs, allowing only authorised personnel to make changes

Dog owner datastore (Store)

This database contains all dog owner data, including their pronoun, first and last name, email address, and physical address.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
125	Unauthorised modification of dog owner data	Tampering	Medium	Mitigated		An attacker might gain unauthorised access and alter the information of the dog owner (e.g., name, email, etc)	* Utilise hashing and checksum mechanisms to detect and prevent unauthorised changes to data * Implement role based access controls to restrict database write permissions to authorised personnel only * Regular audits and integrity checks on the database to identify any unauthorised changes
127	Dog owner datastore unwanted access	Information disclosure	Medium	Mitigated		Sensitive information might be exposed to unauthorised individuals.	* Datastore credentials are securely stored on password vaults with limited set of users having access (apply least privilege principle). * Datastore credentials are injected into connecting software from secured variables or files (apply least privilege principle).
129	Disputed data changes	Repudiation	Medium	Mitigated		An attacker or insider could dispute or deny making changes to records within the datastore, leading to challenges in auditing and accountability.	* Maintain detailed, tamper-evident logs of all actions performed on the datastore, including timestamps, user IDs, and specific changes * Use cryptographic signatures on logs * Restrict access to the datastore and its logs, allowing only authorised personnel to make changes

Send email (Process)

Allows the system to send emails to the dog owner.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
89	Fake emails	Spoofing	Medium	Mitigated		Attackers could send fake emails to the dog owners, leading to confusion and potential security breaches.	* Include specific information in the email that only the council would know (e.g., registration number) * Use domain-based email authentication protocols like SPF, DKIM, and DMARC * Include warnings in legitimate emails about phishing threats and provide a secure method for users to report suspicious emails * Only include secure links with HTTPS

Pay registration fee (Process) - *Out of Scope*

Allows the dog owner to pay for the dog registration.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Manufacture and send new tag (Process)

Manufactures and sends the new dog tag with the new dog tag ID to the dog owner's physical address.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
131	Owner denies receiving tag	Repudiation	Medium	Mitigated		The tag owner may deny having received the tag.	* Logging steps in the manufacturing process, such as completion date * Tracking the package when sending to the owner

Renew dog registration (Process)

Action to renew an existing dog registration.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
130	Impersonation of dog owner	Spoofing	Medium	Open		A dog owner could use someone else's information (email and dog tag ID) to renew the registration of a dog that is not theirs.	
133	User claims to have made payment	Repudiation	Medium	Mitigated		Same as #132	Same as #132
141	Malformed data	Tampering	Medium	Mitigated		Same as #86	Same as #86
145	Adversary in the middle changes the renewal details	Tampering	Medium	Mitigated		An adversary-in-the-middle intercepts the registration renewal details and modifies its content (e.g., address to deliver the new tag to)	* Use secure connection, http-only and secure cookie with unique session id * Sign (hash) content with user's private key
146	Overload request	Denial of service	Medium	Mitigated		Attackers could overload the process by sending a large number of fake or malicious requests.	* Implement rate limiting to prevent DoS attacks * Ensure that backups are available to restore normal operations quickly * Monitor for unusual spikes in traffic and automatically block suspicious activity

Terminate a registration (Process)

Action to terminate an existing dog registration.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	Fraudulent reporting	Spoofing	Medium	Open		A user could obtain another user's email address, dog ID, and dog name, and fraudulently terminate the dog's registration.	
3	Deny terminating registration	Repudiation	Medium	Mitigated		A user could claim that somebody else impersonated them and terminated the dog's registration	* Trace (log) session id, timestamp, originating IP and user id in log. * Validate hashed checksum with end-user's public key. * Send confirmation email (with email log).
4	Flooding of requests from the same IP	Denial of service	Medium	Mitigated		Multiple requests coming from the same IP, or multiple requests to terminate the same dog registration.	* Implement rate limiting to restrict the number of requests that can be processed from the same IP address * Add CAPTCHA to the termination request form to prevent automated bots
139	Malformed data	Tampering	Medium	Mitigated		Same as #86	Same as #86

Declare lost dog (Process)

Action to report a lost dog

Number	Title	Type	Priority	Status	Score	Description	Mitigations
85	Fraudulent reporting	Spoofing	Medium	Open		Attackers may impersonate the dog owner if they know their email address and the dog's name. This can lead to false reports and the attacker also gains the dog's most recent tag ID.	
86	Malformed data	Tampering	Medium	Mitigated		Attackers could pass through specially crafted malformed data, which can lead to denial of service or information disclosure.	* Implement strong input validation and handle unexpected data types * Ensure that a backup mechanism is in place to quickly restore service * Monitor data submissions for signs of DoS attempts in malformed data
87	Overload request	Denial of service	Medium	Mitigated		Attackers could overload the process by sending a large number of fake or malicious requests, leading to a denial of service that prevents legitimate users from reporting lost dogs.	* Implement rate limiting to prevent DoS attacks * Ensure that backups are available to restore normal operations quickly * Monitor for unusual spikes in traffic and automatically block suspicious activity
88	Denial of lost dog report	Repudiation	Medium	Mitigated		Dog owner might later deny having made the lost dog report.	* Send a confirmation email to the email address upon report process completion * Maintain robust and secure logs of all transactions on the app * Provide confirmation page when the report process has been completed

Report found dog (Process)

Action to report a found dog.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
80	False reports	Spoofing	Medium	Open		Anonymous users can get access to the dogs tag number and report the dog as found or report the dog at false locations.	* Use the dog status to find out the dogs, if the owner reported it as LOST. If the status is anything other than LOST don't do anything.
81	Adversary-in-the-Middle - changes the dog tags	Tampering	Medium	Mitigated		An attacker getting access to the network can change the dog tags.	* Validate legitimate dog tags * Encrypt the information while the data is in transit
83	Deny reporting	Repudiation	Medium	Open		An attacker can deny they did not report any dogs.	
84	Endpoint Denial of Service - either with one IP of distributed IPs	Denial of service	Medium	Mitigated		An attacker may report multiple times with the same IP or bot net distributed network to prevent valid reports.	* IP white list and black listing. * Anti DDoS attack services i.e. cloudflare. * Filter Network Traffic using services provided by Content Delivery Networks (CDN).
137	Malformed data	Tampering	Medium	Mitigated		Same as #86	Same as #86

Member of the public (Actor)

Anonymous member of the public.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

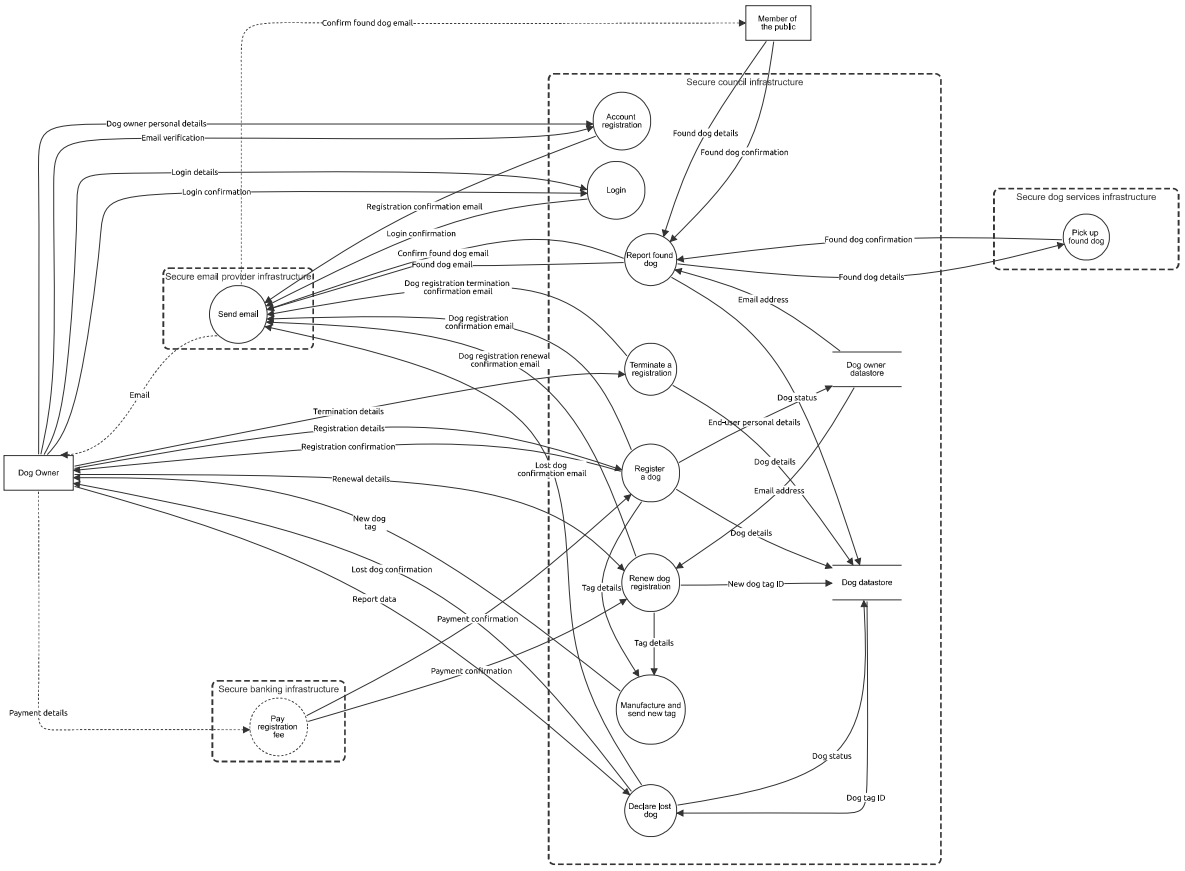
Pick up found dog (Process)

Dog services that are responsible of collecting lost dogs.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

12 Improved system

STRIDE diagram with improvements



12 Improved system

Register a dog (Process)

Action to register a dog.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
64	Register a dog under someone else's name	Elevation of privilege	Medium	Mitigated		A dog owner (whether they have an account or not) could try to register a dog under someone else's name. They would then be able to deny affiliation with the dog.	* Principle of least privilege - only allow logged in users to register their own dogs * Use session IDs to identify logged in users
66	Flooding of requests from the same IP	Denial of service	Medium	Mitigated		User trying to register large numbers of dogs at the same time.	* Add a cooldown time for the same IP to register another dog * Implement rate limiting to restrict the number of requests a single IP address can make * Use CAPTCHA on the registration form to prevent automated bots
132	User claims to have made payment	Repudiation	Medium	Mitigated		The user falsely claims they have paid the registration fee (denies not paying).	* Keep a copy of bank receipts, including the registration number reference and timestamps * Use digital signatures for payment receipts and invoices * Integrate an automated payment gateway that verifies the payments in real-time
140	Malformed data	Tampering	Medium	Mitigated		Same as #86	Same as #86
144	Adversary in the middle changes the registration details	Tampering	Medium	Mitigated		An adversary-in-the-middle intercepts the registration and modifies its content (e.g., email address and physical address)	* Use secure connection, http-only and secure cookie with unique session id * Sign (hash) content with user's private key

Dog Owner (Actor)

A person living in the jurisdiction of the Council who owns one or more dogs.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
167	Weak password	Spoofing	Medium	Mitigated		Attackers guess weak credentials	* Require passwords to be at least 8 characters long and include at least one uppercase letter, one lowercase letter, one number, and one special character.

Dog details (Data Flow)

Includes:
* Dog name
* Dog breed
* Dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations

New dog tag ID (Data Flow)

Includes:
* Old tag ID
* Dogs new tag ID
to replace with the old one

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Tag details (Data Flow)

Includes:
* Dog owners postal address
* Renewed dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations

End-user personal details (Data Flow)

Includes:
* Pronoun
* First and last name
* Email address
* Physical address

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Tag details (Data Flow)

Includes:
* Dog owners postal address
* Unique dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Dog details (Data Flow)

Includes:
- Details of the dog to delete:
* Dogs Tag ID
* Dog name
* Dog breed

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Payment confirmation (Data Flow)

Includes:
- Banking details
  * Account Name
  * Account Number
  * Registration Number

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Registration confirmation (Data Flow)

Includes:
* owner email
*Unique registration number,
*Expiry date for registration

Number	Title	Type	Priority	Status	Score	Description	Mitigations
101	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
109	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Report data (Data Flow)

Includes:
* Email address used to register the dog
* Dog's name

Number	Title	Type	Priority	Status	Score	Description	Mitigations
91	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
105	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Lost dog confirmation (Data Flow)

Includes:
* Dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations
98	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
106	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Dog tag ID (Data Flow)

Includes:
* Dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Email address (Data Flow)

Includes:
* Dog owner's email address

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Dog status (Data Flow)

Includes:
* Dogs new Status : FOUND
* Dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Dog status (Data Flow)

Includes:
* Email address used to register the dog
* Dog's name
* Dog's new status: LOST

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Email address (Data Flow)

Includes:
* Dog owners email address

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Renewal details (Data Flow)

Includes:
* Dog tag ID
* Delivery address

Number	Title	Type	Priority	Status	Score	Description	Mitigations
100	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
108	Insecure connection	Tampering	Medium	Mitigated		Same as #103, an attacker could change the address to steal a dog's tag.	Same as #103

New dog tag (Data Flow)

Includes:
  * Dog owners postal address
  * Renewed dog tag ID

Number	Title	Type	Priority	Status	Score	Description	Mitigations
99	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
107	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Found dog confirmation (Data Flow)

Includes:
  * Dog tag ID
  * Found location

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Registration details (Data Flow)

Includes:
- Personal details:
  * Pronoun
  * First and last name
  * Email address
  * Physical address
- Dog details:
  * Dog name
  * Dog breed

Number	Title	Type	Priority	Status	Score	Description	Mitigations
71	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		An adversary-in-the-middle intercepts the data and reads sensitive information.	* Protect data using TLS * Isolate the communication channels used for transmitting sensitive data * Implement secure communication channels
103	Insecure connection	Tampering	Medium	Mitigated		Data can be tampered by an adversary in the middle where the information can be modified.	* Use TLS to encrypt the data in transit * Implement hashing to create a checksum of the data before transmission and verify it upon receipt * Enforce HTTPS by implementing HSTS, which instructs browsers to only interact with the server over a secure HTTPS connection

Found dog details (Data Flow)

Includes:
  * Dog name
  * Dog breed
  * Dog tag ID
  * Pick up location address

Number	Title	Type	Priority	Status	Score	Description	Mitigations
123	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
124	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Payment confirmation (Data Flow)

Includes:
- Banking details
  * Account Name
  * Account Number
  * Registration Number

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Payment details (Data Flow) - *Out of Scope*

Includes:
- Banking details
  * Account Name
  * Account Number
  * Registration Number

Number	Title	Type	Priority	Status	Score	Description	Mitigations
102	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
104	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Dog owner personal details (Data Flow)

Includes:
  * Email
  * Password
  * First name
  * Last name
  * Pronoun

Number	Title	Type	Priority	Status	Score	Description	Mitigations
153	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
154	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Termination details (Data Flow)

Includes:
  * Email address
  * Dog tag ID
  * Dog name

Number	Title	Type	Priority	Status	Score	Description	Mitigations
63	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
110	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Login details (Data Flow)

Includes:
* Email
* Password

Number	Title	Type	Priority	Status	Score	Description	Mitigations
157	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103
158	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71

Email verification (Data Flow)

User opens unique link given in the confirmation email.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
155	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103
156	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71

Found dog confirmation (Data Flow)

Member of the public clicks on the unique link sent to their email

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Found dog details (Data Flow)

Includes:
* Dog tag ID
* Physical address
* Reporter email
* Image of lost dog

Number	Title	Type	Priority	Status	Score	Description	Mitigations
79	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
147	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Login confirmation (Data Flow)

Includes:
* Unique token to verify login

Number	Title	Type	Priority	Status	Score	Description	Mitigations
159	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103
160	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71

Confirm found dog email (Data Flow)

Email to confirm that a dog has been found by a member of the public. Includes:
* Unique link to confirm that dog has been found

Number	Title	Type	Priority	Status	Score	Description	Mitigations
165	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103
166	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71

Login confirmation (Data Flow)

Includes:
* Unique token to confirm login

Number	Title	Type	Priority	Status	Score	Description	Mitigations
163	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103
164	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71

Registration confirmation email (Data Flow)

Includes:
* Unique link to confirm email

Number	Title	Type	Priority	Status	Score	Description	Mitigations
161	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103
162	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71

Lost dog confirmation email (Data Flow)

Includes:
* Dog tag ID
* Updated dog status

Number	Title	Type	Priority	Status	Score	Description	Mitigations
119	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
120	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Dog registration renewal confirmation email (Data Flow)

Includes:
* Invoice PDF
* Email address

* Email content

Number	Title	Type	Priority	Status	Score	Description	Mitigations
117	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103
118	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71

Dog registration confirmation email (Data Flow)

Includes:
* Invoice PDF (with amount and registration number)
* Email address
* Email content

Number	Title	Type	Priority	Status	Score	Description	Mitigations
115	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
116	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Dog registration termination confirmation email (Data Flow)

Includes:
* Dog owner's email address
* Termination confirmation message
* dog's registration link

Number	Title	Type	Priority	Status	Score	Description	Mitigations
121	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103
122	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71

Found dog email (Data Flow)

Includes:
* Dog owner's email address
* Dog tag ID
* Dog found message

Number	Title	Type	Priority	Status	Score	Description	Mitigations
112	Adversary-in-the-middle gain information	Information disclosure	Medium	Mitigated		Same as #71	Same as #71
113	Insecure connection	Tampering	Medium	Mitigated		Same as #103	Same as #103

Email (Data Flow) - *Out of Scope*

Email containing the relevant information.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Confirm found dog email (Data Flow) - *Out of Scope*

Email containing the unique link that the member of the public clicks on to confirm the dog has been found.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Dog datastore (Store)

This database contains the details of the dogs, including their name, breed, status, registration number, expiry date, tag ID, and owner.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	Unauthorised modification of dog data	Tampering	Medium	Mitigated		An attacker might gain unauthorised access and alter the information of the dog (e.g., name, lost status, owner, dog tag ID).	* Utilise hashing and checksum mechanisms to detect and prevent unauthorised changes to data * Implement role based access controls to restrict database write permissions to authorised personnel only * Regular audits and integrity checks on the database to identify any unauthorised changes
6	Dog datastore unwanted access	Information disclosure	Medium	Mitigated		Sensitive information might be exposed to unauthorised individuals.	* Datastore credentials are securely stored on password vaults with limited set of users having access (apply least privilege principle). * Datastore credentials are injected into connecting software from secured variables or files (apply least privilege principle).
7	Disputed data changes	Repudiation	Medium	Mitigated		An attacker or insider could dispute or deny making changes to records within the datastore, leading to challenges in auditing and accountability.	* Maintain detailed, tamper-evident logs of all actions performed on the datastore, including timestamps, user IDs, and specific changes * Use cryptographic signatures on logs * Restrict access to the datastore and its logs, allowing only authorised personnel to make changes

Dog owner datastore (Store)

This database contains all dog owner data, including their pronoun, first and last name, email address, and physical address.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
125	Unauthorised modification of dog owner data	Tampering	Medium	Mitigated		An attacker might gain unauthorised access and alter the information of the dog owner (e.g., name, email, etc)	* Utilise hashing and checksum mechanisms to detect and prevent unauthorised changes to data * Implement role based access controls to restrict database write permissions to authorised personnel only * Regular audits and integrity checks on the database to identify any unauthorised changes

Number	Title	Type	Priority	Status	Score	Description	Mitigations
127	Dog owner datastore unwanted access	Information disclosure	Medium	Mitigated		Sensitive information might be exposed to unauthorised individuals.	* Datastore credentials are securely stored on password vaults with limited set of users having access (apply least privilege principle). * Datastore credentials are injected into connecting software from secured variables or files (apply least privilege principle).
129	Disputed data changes	Repudiation	Medium	Mitigated		An attacker or insider could dispute or deny making changes to records within the datastore, leading to challenges in auditing and accountability.	* Maintain detailed, tamper-evident logs of all actions performed on the datastore, including timestamps, user IDs, and specific changes * Use cryptographic signatures on logs * Restrict access to the datastore and its logs, allowing only authorised personnel to make changes

Send email (Process)

Allows the system to send emails to the dog owner.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
89	Fake emails	Spoofing	Medium	Mitigated		Attackers could send fake emails to the dog owners, leading to confusion and potential security breaches.	* Include specific information in the email that only the council would know (e.g., registration number) * Use domain-based email authentication protocols like SPF, DKIM, and DMARC * Include warnings in legitimate emails about phishing threats and provide a secure method for users to report suspicious emails * Only include secure links with HTTPS

Pay registration fee (Process) - *Out of Scope*

Allows the dog owner to pay for the dog registration.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Manufacture and send new tag (Process)

Manufactures and sends the new dog tag with the new dog tag ID to the dog owner's physical address.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
131	Owner denies receiving tag	Repudiation	Medium	Mitigated		The tag owner may deny having received the tag.	* Logging steps in the manufacturing process, such as completion date * Tracking the package when sending to the owner

Renew dog registration (Process)

Action to renew an existing dog registration.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
130	Attempt to renew someone else's dog registration	Elevation of privilege	Medium	Mitigated		An attacker could try to renew the registration of a dog they do not own, causing the system to spam the owner's email.	* Principle of least privilege - only allow users to renew their own dogs' registrations * Use session IDs to keep track of logged in users
133	User claims to have made payment	Repudiation	Medium	Mitigated		Same as #132	Same as #132
141	Malformed data	Tampering	Medium	Mitigated		Same as #86	Same as #86
145	Adversary in the middle changes the renewal details	Tampering	Medium	Mitigated		An adversary-in-the-middle intercepts the registration renewal details and modifies its content (e.g., address to deliver the new tag to)	* Use secure connection, http-only and secure cookie with unique session id * Sign (hash) content with user's private key
146	Overload request	Denial of service	Medium	Mitigated		Attackers could overload the process by sending a large number of fake or malicious requests.	* Implement rate limiting to prevent DoS attacks * Ensure that backups are available to restore normal operations quickly * Monitor for unusual spikes in traffic and automatically block suspicious activity

Terminate a registration (Process)

Action to terminate an existing dog registration.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	Terminate some else's dog registration	Elevation of privilege	Medium	Mitigated		A user could terminate the dog registration that is owned by someone else.	* Principle of least privilege - only allow the dog's owner to terminate the registration. * Give a unique session id when logging in to check the identity of the user.
3	Deny terminating registration	Repudiation	Medium	Mitigated		A user could claim that somebody else impersonated them and terminated the dog's registration	* Trace (log) session id, timestamp, originating IP and user id in log. * Validate hashed checksum with end-user's public key. * Send confirmation email (with email log).
4	Flooding of requests from the same IP	Denial of service	Medium	Mitigated		Multiple requests coming from the same IP, or multiple requests to terminate the same dog registration.	* Implement rate limiting to restrict the number of requests that can be processed from the same IP address * Add CAPTCHA to the termination request form to prevent automated bots
139	Malformed data	Tampering	Medium	Mitigated		Same as #86	Same as #86

Declare lost dog (Process)

Action to report a lost dog

Number	Title	Type	Priority	Status	Score	Description	Mitigations
85	Report some else's dog as lost	Elevation of privilege	Medium	Mitigated		Attackers may try to declare someone else's dog as lost.	* Principle of least privilege - only allow users to declare their own dogs as lost * Use session IDs to keep track of logged in users
86	Malformed data	Tampering	Medium	Mitigated		Attackers could pass through specially crafted malformed data, which can lead to denial of service or information disclosure.	* Implement strong input validation and handle unexpected data types * Ensure that a backup mechanism is in place to quickly restore service * Monitor data submissions for signs of DoS attempts in malformed data
87	Overload request	Denial of service	Medium	Mitigated		Attackers could overload the process by sending a large number of fake or malicious requests, leading to a denial of service that prevents legitimate users from reporting lost dogs.	* Implement rate limiting to prevent DoS attacks * Ensure that backups are available to restore normal operations quickly * Monitor for unusual spikes in traffic and automatically block suspicious activity
88	Denial of lost dog report	Repudiation	Medium	Mitigated		Dog owner might later deny having made the lost dog report.	* Send a confirmation email to the email address upon report process completion * Maintain robust and secure logs of all transactions on the app * Provide confirmation page when the report process has been completed

Report found dog (Process)

Action to report a found dog.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
80	False reports	Spoofing	Medium	Mitigated		Anonymous users can get access to the dogs tag number and report the dog as found or report the dog at false locations.	* Check the dog's current status - if the owner reported it as LOST, then send the dog services. If the status is anything other than LOST, email the dog owner to confirm whether the dog is actually lost. * Require all reports to include an image of the found dog's tag, which is then manually checked by a council member. * Flag email accounts that are used for multiple false reports and ignore future reports from them.
81	Adversary-in-the-Middle - changes the dog tags	Tampering	Medium	Mitigated		An attacker getting access to the network can change the dog tags.	* Validate legitimate dog tags * Encrypt the information while the data is in transit
83	Deny reporting	Repudiation	Medium	Mitigated		An attacker can deny they reported any dogs.	* Require all reports to be confirmed by emailing the reporter a verification link * Keep a log of the email used for each report

Number	Title	Type	Priority	Status	Score	Description	Mitigations
84	Endpoint Denial of Service - either with one IP of distributed IPs	Denial of service	Medium	Mitigated		An attacker may report multiple times with the same IP or bot net distributed network to prevent valid reports.	* IP white list and black listing. * Anti DDoS attack services i.e. cloudflare. * Filter Network Traffic using services provided by Content Delivery Networks (CDN).
137	Malformed data	Tampering	Medium	Mitigated		Same as #86	Same as #86

Member of the public (Actor)

Anonymous member of the public.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Pick up found dog (Process)

Dog services that are responsible of collecting lost dogs.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Account registration (Process)

Action to register as a dog owner.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
148	Register an account as someone else	Spoofing	Medium	Mitigated		A user could register an account as someone else.	* Require users to click a unique link (which is sent via email) to finish registering.
149	Flooding of requests from the same IP	Denial of service	Medium	Mitigated		A user trying to register large numbers of owner accounts at the same time.	* Add a cooldown time for the same IP to register another dog * Implement rate limiting to restrict the number of requests a single IP address can make * Use CAPTCHA on the registration form to prevent automated bots

Login (Process)

Action for a dog owner to log in.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
150	Logging in as someone else	Spoofing	Medium	Mitigated		A user could try to log in with stolen credentials, or brute-force the password.	* Require two-factor email authentication whenever a user logs in from a new browser. * After 5 consecutive incorrect guesses, lock the account for 30 seconds.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
152	Multiple automated requests	Denial of service	Medium	Mitigated		Automated tools could send large amounts of requests to the site to slow down or crash the system.	* Use CAPTCHA challenges to confirm that the user is human * Add time-outs for IPs that send too many requests at the same time