Threat Analysis of Council Building Consent Application Management System

Owner: Bede Skinner-Vennell, Luke Garside, Sam Clark
Reviewer:
Contributors: Bede Skinner-Vennell, Luke Garside, Sam Clark
Date Generated: Fri Aug 18 2023

Executive Summary

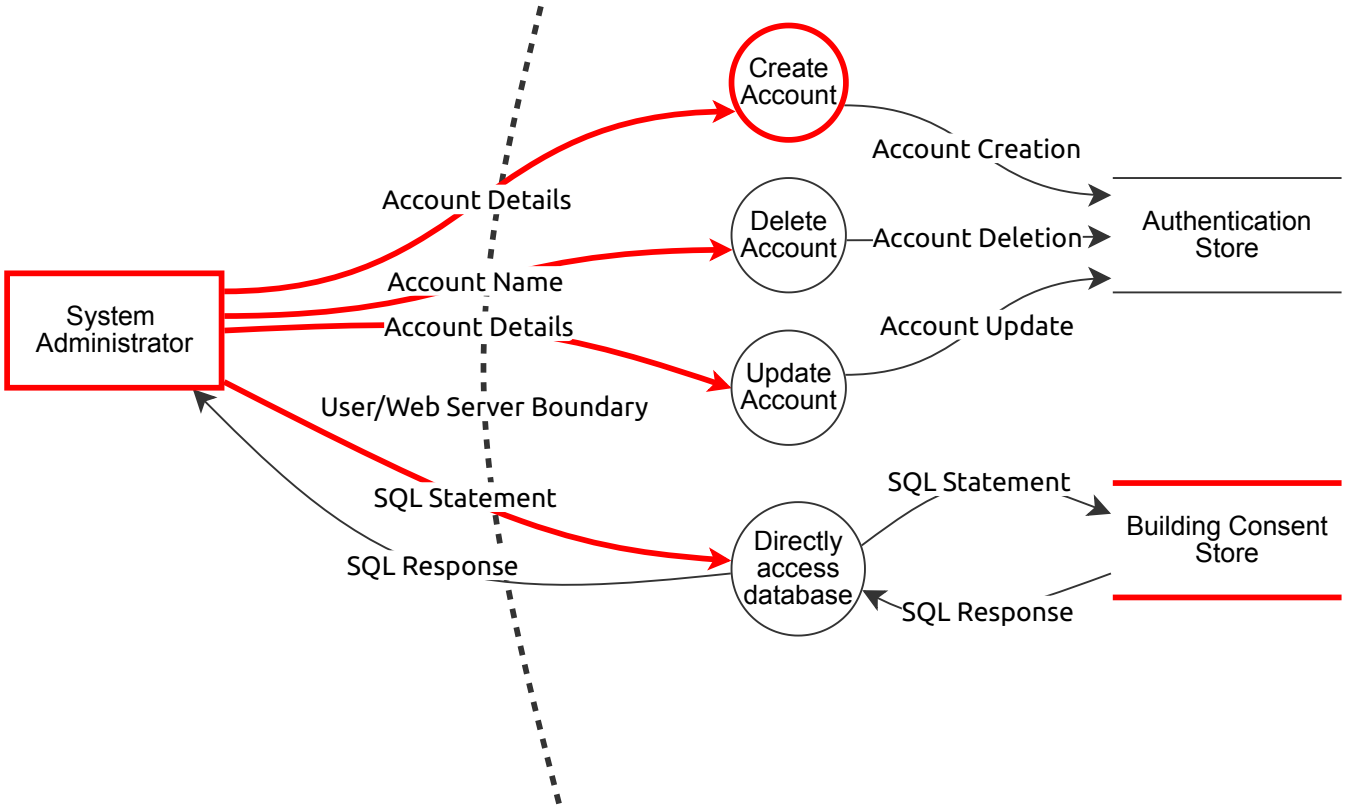
High level system description

Not provided

Summary

Total Threats	165
Total Mitigated	95
Not Mitigated	70
Open / High Priority	0
Open / Medium Priority	70
Open / Low Priority	0
Open / Unknown Priority	0

admin


Create Account
Account Creation
Account Details
Delete Account
Account Deletion
Authentication Store
Account Name
System Administrator
Account Details
Account Update
Update Account
User/Web Server Boundary
SQL Statement
SQL Statement
Building Consent Store
Directly access database
SQL Response
SQL Response

admin

SQL Statement (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SQL Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Account Update (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Account Creation (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Account Deletion (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Account Details (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
127	Adversary in the Middle Attack	Tampering	Medium	Mitigated		Threat actor intercepts network traffic with the staff member's user details	Encrypt all network communication and use transport layer security

Number	Title	Type	Priority	Status	Score	Description	Mitigations
128	Denial of Service From Repeated Requests	Denial of service	Medium	Open		A malicious actor repeatedly sends requests to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, you could put staff logins behind a firewall and only allow access from the local council network or through a secure VPN. However, this is not feasible in the current system as there is a requirement for the website to be publicly available.

Account Details (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
131	Denial of Service From Repeated Access Attempts	Denial of service	Medium	Open		A malicious actor repeatedly attempts to login to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, you could put staff logins behind a firewall and only allow access from the local council network or through a secure VPN. However, this is not feasible in the current system as there is a requirement for the website to be publicly available.
132	Adversary in the Middle Attack	Tampering	Medium	Mitigated		Threat actor intercepts network traffic with the staff member's details	Mitigated - Encrypt all network communication and use transport layer security

SQL Statement (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
134	Adversary in the Middle Attack	Tampering	Medium	Mitigated		If a threat actor intercepts the network packets meant for the system, they could edit the intended action to be malicious.	Encrypt all network communication and use transport layer security
136	Repeated Requests	Denial of service	Medium	Open		If a threat actor made repeated or large requests to the database, it could slow down or freeze access for other users.	Require confirmation for large requests. Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, you could put staff logins behind a firewall and only allow access from the local council network or through a secure VPN. However, this is not feasible in the current system as there is a requirement for the website to be publicly available.

SQL Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
141	Adversary in the Middle Attack	Tampering	Medium	Mitigated		If a threat actor intercepts the network packets meant for the user, they could access private information.	Encrypt all network communication and use transport layer security

Account Name (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
129	Adversary in the Middle Attack	Tampering	Medium	Mitigated		Threat actor intercepts network traffic with the staff member's user details	Mitigated - Encrypt all network communication and use transport layer security
130	Denial of Service From Repeated Access Attempts	Denial of service	Medium	Open		A malicious actor repeatedly attempts to access the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, you could put staff logins behind a firewall and only allow access from the local council network or through a secure VPN. However, this is not feasible in the current system as there is a requirement for the website to be publicly available.

System Administrator (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
124	Staff Credentials Stolen	Spoofing	Medium	Open		Staff credentials can be stolen via methods including brute force attacks, man in the middle attacks, them writing their details on a sticky note on their monitor, etc	Require two factor authentication and passwords that contain at least 10 characters, including at least one of each of upper case letter, lower case letter, number, and special character. Provide training to staff on best practices for password security.
125	Staff Session Hijacked	Spoofing	Medium	Open		Staff session tokens get stolen by a threat actor and used maliciously to use the application as the staff member.	Use secure cookies with a session token sufficient length and entropy (128 bits long and at 64 bits of entropy). Also provide staff with training on avoiding phishing attacks and use email filters.
126	Spoofed Account Performing Malicious Actions	Repudiation	Medium	Mitigated		Accounts that have been spoofed can perform malicious acts without being able to prove whether the account was stolen by a threat actor.	Log all actions taken by actors, including login attempts with the actor's ip address, to ensure that the source of actions can be traced back to the actor that initiated them.

Create Account (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
142	Repeated Requests	Denial of service	Medium	Open		Repeated requests by an actor use significant resources such as CPU and memory	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, you could put staff pages behind a firewall and only allow access from the local council network or through a secure VPN. However, this is not feasible in the current system as there is a requirement for the website to be publicly available.
146	Denying User Creation	Repudiation	Medium	Mitigated		Log all interactions with the system, including the ip address of the actor, and their account details.	Log all interactions with the system, including the ip address of the actor, and their account details.

Delete

Account (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
147	Denying User Deletion	Repudiation	Medium	Mitigated		A threat actor could delete a user and deny they did it	Log all interactions with the system, including the ip address of the actor, and their account details.

Update Account (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Directly access database (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authentication Store (Store)

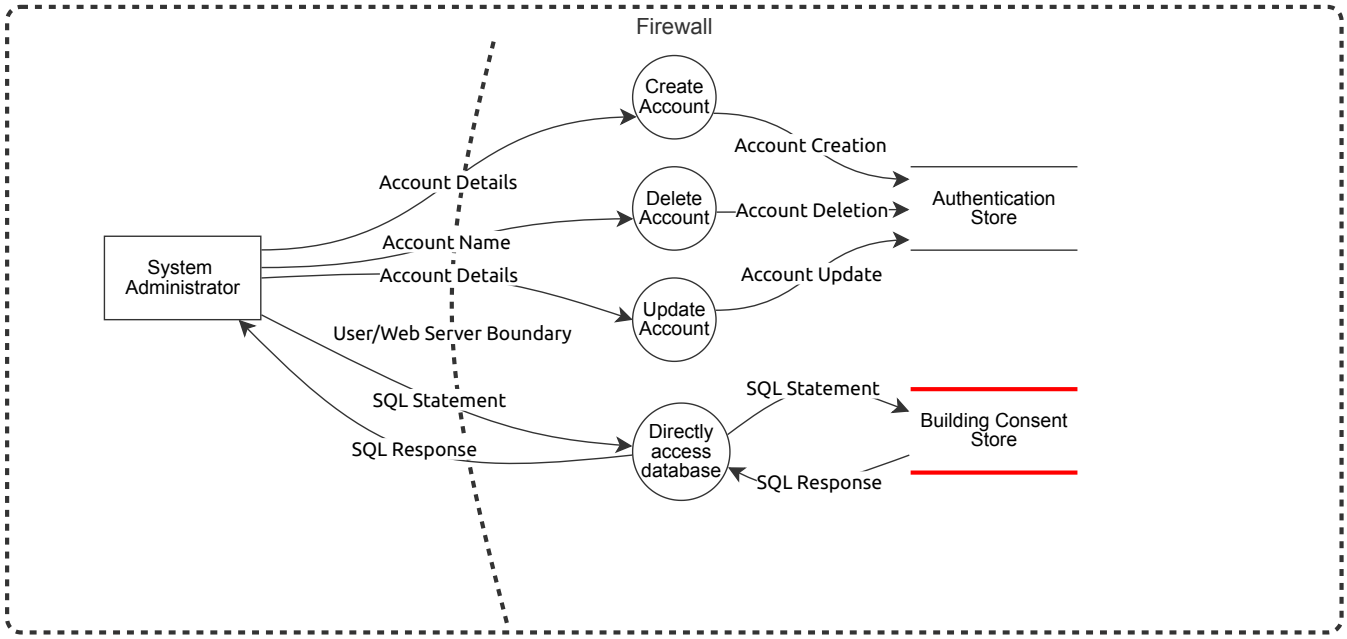
Number	Title	Type	Priority	Status	Score	Description	Mitigations
56	Database Filling Up	Denial of service	Medium	Mitigated		If too many users are registered, issues could occur due to the database filling up	This is mitigated by only allowing users to be created by administrators. Checks are performed before adding a new user account to ensure the database has enough space.

Building Consent Store (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
148	Data Leak	Information disclosure	Medium	Open		Private data could be leaked from the system	Secure database access behind a firewall and access control

admin - firewall

An updated version of the admin diagram where staff members can only access the system inside the council's network or using a secure VPN



admin - firewall

SQL Statement (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SQL Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Account Update (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Account Creation (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Account Deletion (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SQL Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
141	Adversary in the Middle Attack	Tampering	Medium	Mitigated		If a threat actor intercepts the network packets meant for the user, they could access private information.	Encrypt all network communication and use transport layer security

Account Name (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
129	Adversary in the Middle Attack	Tampering	Medium	Mitigated		Threat actor intercepts network traffic with the staff member's user details	Mitigated - Encrypt all network communication and use transport layer security
130	Denial of Service From Repeated Access Attempts	Denial of service	Medium	Mitigated		A malicious actor repeatedly attempts to access the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, staff logins are put behind a firewall and only allowed access from the local council network or through a secure VPN.

Account Details (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
127	Adversary in the Middle Attack	Tampering	Medium	Mitigated		Threat actor intercepts network traffic with the staff member's user details	Encrypt all network communication and use transport layer security
128	Denial of Service From Repeated Requests	Denial of service	Medium	Mitigated		A malicious actor repeatedly sends requests to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, staff logins are put behind a firewall and only allowed access from the local council network or through a secure VPN.

Account Details (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
131	Denial of Service From Repeated Access Attempts	Denial of service	Medium	Mitigated		A malicious actor repeatedly attempts to login to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, staff logins are put behind a firewall and only allowed access from the local council network or through a secure VPN.
132	Adversary in the Middle Attack	Tampering	Medium	Mitigated		Threat actor intercepts network traffic with the staff member's details	Mitigated - Encrypt all network communication and use transport layer security

SQL Statement (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
134	Adversary in the Middle Attack	Tampering	Medium	Mitigated		If a threat actor intercepts the network packets meant for the system, they could edit the intended action to be malicious.	Encrypt all network communication and use transport layer security

Number	Title	Type	Priority	Status	Score	Description	Mitigations
136	Repeated Requests	Denial of service	Medium	Mitigated		If a threat actor made repeated or large requests to the database, it could slow down or freeze access for other users.	Require confirmation for large requests. Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, staff logins are put behind a firewall and only allowed access from the local council network or through a secure VPN.

System Administrator (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
124	Staff Credentials Stolen	Spoofing	Medium	Mitigated		Staff credentials can be stolen via methods including brute force attacks, man in the middle attacks, them writing their details on a sticky note on their monitor, etc	Require two factor authentication and passwords that contain at least 10 characters, including at least one of each of upper case letter, lower case letter, number, and special character. Provide training to staff on best practices for password security. Additionally, staff logins are put behind a firewall and only allowed access from the local council network or through a secure VPN.
125	Staff Session Hijacked	Spoofing	Medium	Mitigated		Staff session tokens get stolen by a threat actor and used maliciously to use the application as the staff member.	Use secure cookies with a session token sufficient length and entropy (128 bits long and at 64 bits of entropy). Also provide staff with training on avoiding phishing attacks and use email filters. Additionally, staff logins are put behind a firewall and only allowed access from the local council network or through a secure VPN.
126	Spoofed Account Performing Malicious Actions	Repudiation	Medium	Mitigated		Accounts that have been spoofed can perform malicious acts without being able to prove whether the account was stolen by a threat actor.	Log all actions taken by actors, including login attempts with the actor's ip address, to ensure that the source of actions can be traced back to the actor that initiated them.

Create Account (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
142	Repeated Requests	Denial of service	Medium	Mitigated		Repeated requests by an actor use significant resources such as CPU and memory	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, staff logins are put behind a firewall and only allowed access from the local council network or through a secure VPN.
146	Denying User Creation	Repudiation	Medium	Mitigated		Log all interactions with the system, including the ip address of the actor, and their account details.	Log all interactions with the system, including the ip address of the actor, and their account details.

Delete Account (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
147	Denying User Deletion	Repudiation	Medium	Mitigated		A threat actor could delete a user and deny they did it	Log all interactions with the system, including the ip address of the actor, and their account details.

Update Account (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Directly access database (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

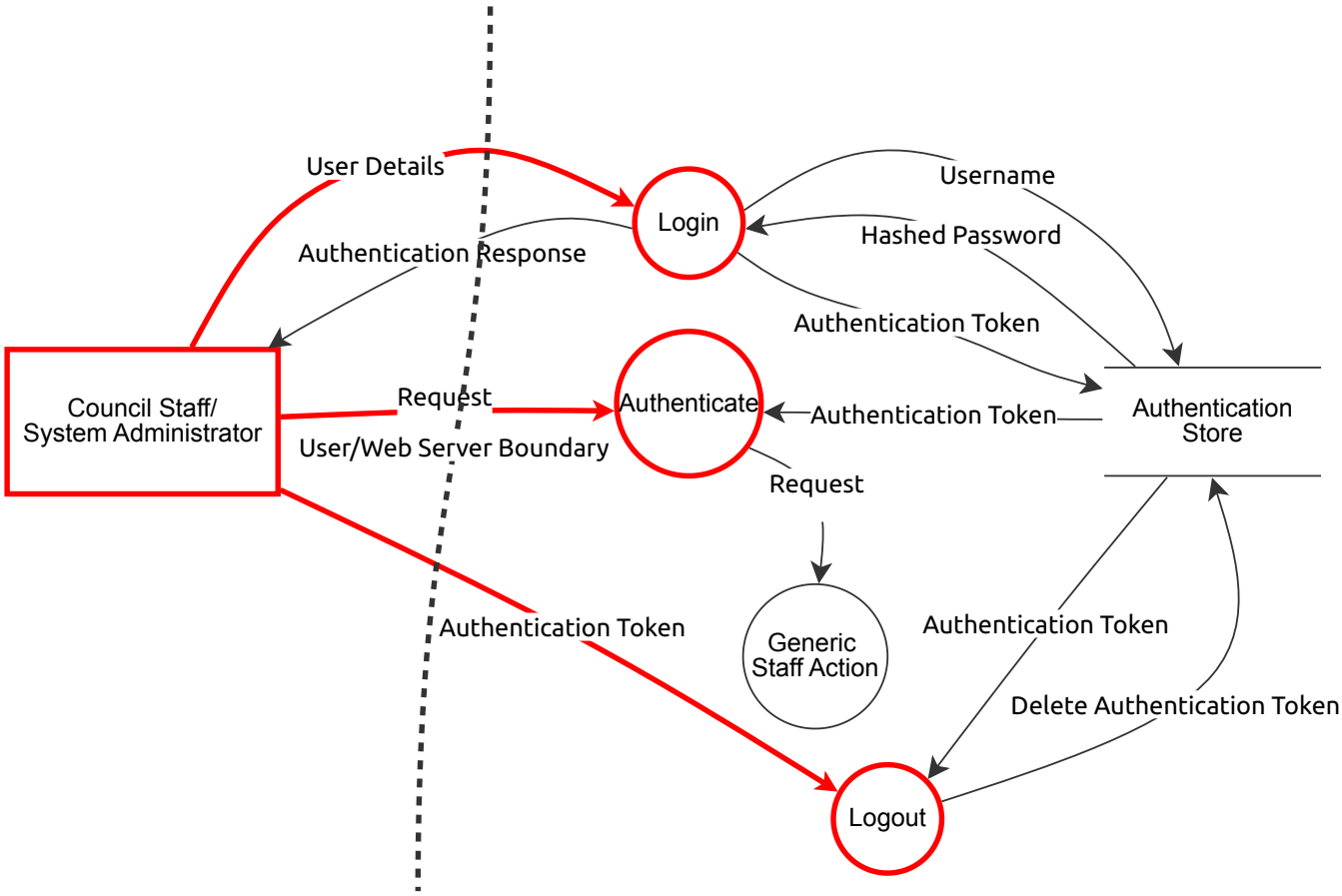
Authentication Store (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
56	Database Filling Up	Denial of service	Medium	Mitigated		If too many users are registered, issues could occur due to the database filling up	This is mitigated by only allowing users to be created by administrators. Checks are performed before adding a new user account to ensure the database has enough space.

Building Consent Store (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
148	Data Leak	Information disclosure	Medium	Open		Private data could be leaked from the system	Secure database access behind a firewall and access control

login


User Details
Login
Username
Hashed Password
Authentication Response
Authentication Token
Council Staff/
System Administrator
Request
Authenticate
Authentication Token
Authentication
Store
User/Web Server Boundary
Request
Authentication Token
Generic
Staff Action
Authentication Token
Delete Authentication Token
Logout

login

Council Staff/ System Administrator (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	Staff Credentials Stolen	Spoofing	Medium	Open		Staff credentials can be stolen via methods including brute force attacks, man in the middle attacks, them writing their details on a sticky note on their monitor, etc	Require two factor authentication and passwords that contain at least 10 characters, including at least one of each of upper case letter, lower case letter, number, and special character. Provide training to staff on best practices for password security.
3	Staff Session Hijacked	Spoofing	Medium	Open		Staff session tokens get stolen by a threat actor and used maliciously to use the application as the staff member.	Use secure cookies with a session token sufficient length and entropy (128 bits long and at 64 bits of entropy). Also provide staff with training on avoiding phishing attacks and use email filters.
4	Spoofed Account Performing Malicious Actions	Repudiation	Medium	Mitigated		Accounts that have been spoofed can perform malicious acts without being able to prove whether the account was stolen by a threat actor.	Log all actions taken by actors, including login attempts with the actor's ip address, to ensure that the source of actions can be traced back to the actor that initiated them.

Authentication Token (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authentication Token (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Delete Authentication Token (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authentication Token (Data Flow)

Auth token with a 1 week timeout

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Hashed Password (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Username (Data Flow)

Request the hashed password for the given username

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authentication Response (Data Flow)

Either an authentication token with a 1 week timeout (if login successful), or a message saying login details were incorrect, but not specifying why (if not)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
9	Disclosure of Used Usernames	Information disclosure	Medium	Mitigated		When the actor supplies an incorrect or invalid username or password, they can determine whether the username is used in the system because the feedback specifies which field is invalid.	Only provide generic feedback stating that the username or password is incorrect.

User Details (Data Flow)

Username and password

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	Network Tampering (Adversary in the Middle Attack)	Tampering	Medium	Mitigated		Threat actor intercepts network traffic with the staff member's user details	Mitigated - Encrypt all network communication and use transport layer security
11	Denial of Service From Repeated Login Attempts	Denial of service	Medium	Open		A malicious actor repeatedly attempts to login to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, you could put staff logins behind a firewall and only allow access from the local council network or through a secure VPN. However, this is not feasible in the current system as there is a requirement for the website to be publicly available.

Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
34	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the system, modify the intended action, then forward it to the system.	Require HTTPS and transport layer security.
36	Repeated Requests	Denial of service	Medium	Open		A malicious actor repeatedly sends requests to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, you could put staff pages behind a firewall and only allow access from the local council network or through a secure VPN. However, this is not feasible in the current system as there is a requirement for the website to be publicly available.

Authentication Token (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
52	Repeated Requests	Denial of service	Medium	Open		A malicious actor repeatedly sends requests to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, you could put staff pages behind a firewall and only allow access from the local council network or through a secure VPN. However, this is not feasible in the current system as there is a requirement for the website to be publicly available.
55	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the system, steal the authentication token, then discard the packet so the logout request is not completed. The threat actor then has a authentication token for a staff member.	Require HTTPS and transport layer security.

Authentication Store (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	Data Tampering	Tampering	Medium	Mitigated		An actor gains access to the authentication store and alters or removes entries	Store database credentials in a secure location and not in plain text. Store user credentials in an encrypted form. Again use the least privileged principle. Also only allow read access to the database from the login endpoint.
15	Visibility of Restricted Data	Information disclosure	Medium	Mitigated		Staff members should not be able to see information about other actors credentials.	Apply the least privileged principle to ensure the minimum amount data is visible.

Logout (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
53	Repeated Requests	Denial of service	Medium	Open		A malicious actor repeatedly sends requests to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, you could put staff pages behind a firewall and only allow access from the local council network or through a secure VPN. However, this is not feasible in the current system as there is a requirement for the website to be publicly available.

Login (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
26	Stealing Credentials with Fake Login Page	Spoofing	Medium	Open		A threat actor creates a fake login page resembling the real login page. This is then used to trick staff members into sharing their login details with the threat actor.	Purchase similar domain names so that threat actors can't use them. Use a simple domain name so it's easier for the users to identify.
29	Disclosure of Used Usernames	Information disclosure	Medium	Mitigated		When the actor supplies an incorrect or invalid username or password, they can determine whether the username is used in the system because the feedback specifies which field is invalid.	Only provide generic feedback stating that the username or password is incorrect.
30	Repeated Login Attempts	Denial of service	Medium	Open		Repeated login attempts by an actor use significant resources such as CPU and memory	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, you could put staff pages behind a firewall and only allow access from the local council network or through a secure VPN. However, this is not feasible in the current system as there is a requirement for the website to be publicly available.
31	Distributed Denial of Service Attack	Denial of service	Medium	Open		Similarly to the repeated login attempts, a distributed denial of service attack can cause significant CPU and memory usage. It can be hard to mitigate because requests come from lots of different sources, so can't all be blocked.	Use an access control list and scale up server capacity to allow for more concurrent requests. It is assumed that this is managed by the cloud service provider. Additionally, you could put staff logins behind a firewall and only allow access from the local council network or through a secure VPN. However, this is not feasible in the current system as there is a requirement for the website to be publicly available.
32	SQL Injection	Elevation of privilege	Medium	Mitigated		When user inputs are not sanitised and handled correctly by the process, it can lead to malicious actions being performed within the process, leading the threat actor performing actions they don't have the privileges to do.	Sanitise user input so that it can't be executed as code.

Authenticate (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

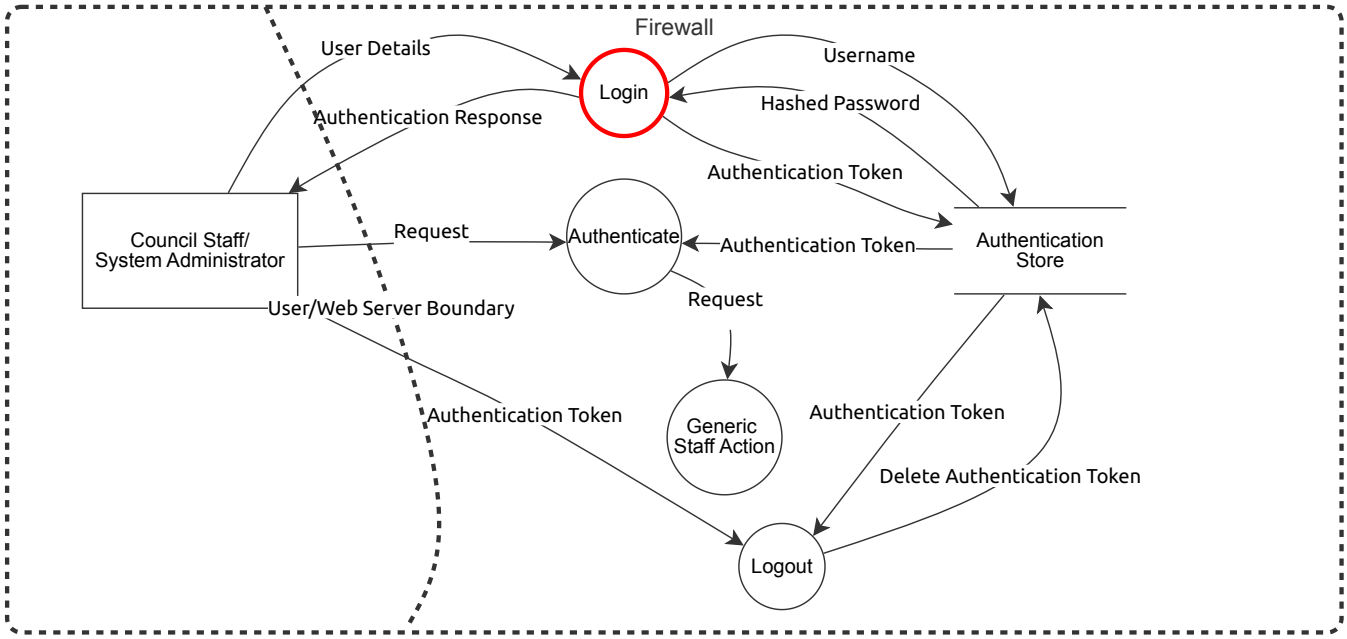
Number	Title	Type	Priority	Status	Score	Description	Mitigations
40	Session Hijacking	Spoofing	Medium	Open		Staff session tokens get stolen by a threat actor and used maliciously to use the application as the staff member.	Use secure cookies with a session token sufficient length and entropy (128 bits long and at 64 bits of entropy). Also provide staff with training on avoiding phishing attacks and use email filters.
48	Repeated Requests	Denial of service	Medium	Open		Repeated request attempts by an actor use significant resources such as CPU and memory	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, you could put staff pages behind a firewall and only allow access from the local council network or through a secure VPN. However, this is not feasible in the current system as there is a requirement for the website to be publicly available.
51	Performing Actions Above Privilege Level	Elevation of privilege	Medium	Mitigated		By failing to restrict administration actions, staff members could perform actions above their privilege level.	Implement role based authorisation for all system actions.

Generic
Staff Action (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

login - firewall

An updated version of the login diagram where staff members can only access the system inside the council's network or using a secure VPN



login - firewall

Council Staff/ System Administrator (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	Staff Credentials Stolen	Spoofing	Medium	Mitigated		Staff credentials can be stolen via methods including brute force attacks, man in the middle attacks, them writing their details on a sticky note on their monitor, etc	Require two factor authentication and passwords that contain at least 10 characters, including at least one of each of upper case letter, lower case letter, number, and special character. Provide training to staff on best practices for password security. This is also mitigated by all access to the system being behind a firewall
3	Staff Session Hijacked	Spoofing	Medium	Mitigated		Staff session tokens get stolen by a threat actor and used maliciously to use the application as the staff member.	Use secure cookies with a session token sufficient length and entropy (128 bits long and at 64 bits of entropy). Also provide staff with training on avoiding phishing attacks and use email filters. This is also mitigated by all access to the system being behind a firewall
4	Spoofed Account Performing Malicious Actions	Repudiation	Medium	Mitigated		Accounts that have been spoofed can perform malicious acts without being able to prove whether the account was stolen by a threat actor.	Log all actions taken by actors, including login attempts with the actor's ip address, to ensure that the source of actions can be traced back to the actor that initiated them.

Authentication Token (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authentication Token (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Delete Authentication Token (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authentication Token (Data Flow)

Auth token with a 1 week timeout

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Hashed Password (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Username (Data Flow)

Request the hashed password for the given username

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authentication Response (Data Flow)

Either an authentication token with a 1 week timeout (if login successful), or a message saying login details were incorrect, but not specifying why (if not)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
9	Disclosure of Used Usernames	Information disclosure	Medium	Mitigated		When the actor supplies an incorrect or invalid username or password, they can determine whether the username is used in the system because the feedback specifies which field is invalid.	Only provide generic feedback stating that the username or password is incorrect.

Authentication Token (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
52	Repeated Requests	Denial of service	Medium	Mitigated		A malicious actor repeatedly sends requests to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, staff pages are behind a firewall and only allow access from the local council network or through a secure VPN.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
55	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the system, steal the authentication token, then discard the packet so the logout request is not completed. The threat actor then has a authentication token for a staff member.	Require HTTPS and transport layer security.

Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
34	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the system, modify the intended action, then forward it to the system.	Require HTTPS and transport layer security.
36	Repeated Requests	Denial of service	Medium	Mitigated		A malicious actor repeatedly sends requests to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, staff pages are behind a firewall and only allow access from the local council network or through a secure VPN.

User Details (Data Flow)

Username and password

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	Network Tampering (Adversary in the Middle Attack)	Tampering	Medium	Mitigated		Threat actor intercepts network traffic with the staff member's user details	Mitigated - Encrypt all network communication and use transport layer security
11	Denial of Service From Repeated Login Attempts	Denial of service	Medium	Mitigated		A malicious actor repeatedly attempts to login to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, staff pages are behind a firewall and only allow access from the local council network or through a secure VPN.

Authentication Store (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
12	Data Tampering	Tampering	Medium	Mitigated		An actor gains access to the authentication store and alters or removes entries	Store database credentials in a secure location and not in plain text. Store user credentials in an encrypted form. Again use the least privileged principle. Also only allow read access to the database from the login endpoint.
15	Visibility of Restricted Data	Information disclosure	Medium	Mitigated		Staff members should not be able to see information about other actors credentials.	Apply the least privileged principle to ensure the minimum amount data is visible.

Logout (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
53	Repeated Requests	Denial of service	Medium	Mitigated		A malicious actor repeatedly sends requests to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, staff pages are behind a firewall and access is only allowed from the local council network or through a secure VPN. This prevents denial of service attacks from external actors.

Login (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
26	Stealing Credentials with Fake Login Page	Spoofing	Medium	Open		A threat actor creates a fake login page resembling the real login page. This is then used to trick staff members into sharing their login details with the threat actor.	Purchase similar domain names so that threat actors can't use them. Use a simple domain name so it's easier for the users to identify.
29	Disclosure of Used Usernames	Information disclosure	Medium	Mitigated		When the actor supplies an incorrect or invalid username or password, they can determine whether the username is used in the system because the feedback specifies which field is invalid.	Only provide generic feedback stating that the username or password is incorrect.
30	Repeated Login Attempts	Denial of service	Medium	Mitigated		Repeated login attempts by a malicious actor use significant resources such as CPU and memory	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, staff pages are behind a firewall and access is only allowed from the local council network or through a secure VPN. This prevents denial of service attacks from external actors.
31	Distributed Denial of Service Attack	Denial of service	Medium	Mitigated		Similarly to the repeated login attempts, a distributed denial of service attack can cause significant CPU and memory usage. It can be hard to mitigate because requests come from lots of different sources, so can't all be blocked.	Staff logins are behind a firewall and access is only allowed from the local council network or through a secure VPN.
32	SQL Injection	Elevation of privilege	Medium	Mitigated		When user inputs are not sanitised and handled correctly by the process, it can lead to malicious actions being performed within the process, leading the threat actor performing actions they don't have the privileges to do.	Sanitise user input so that it can't be executed as code.

Authenticate (Process)

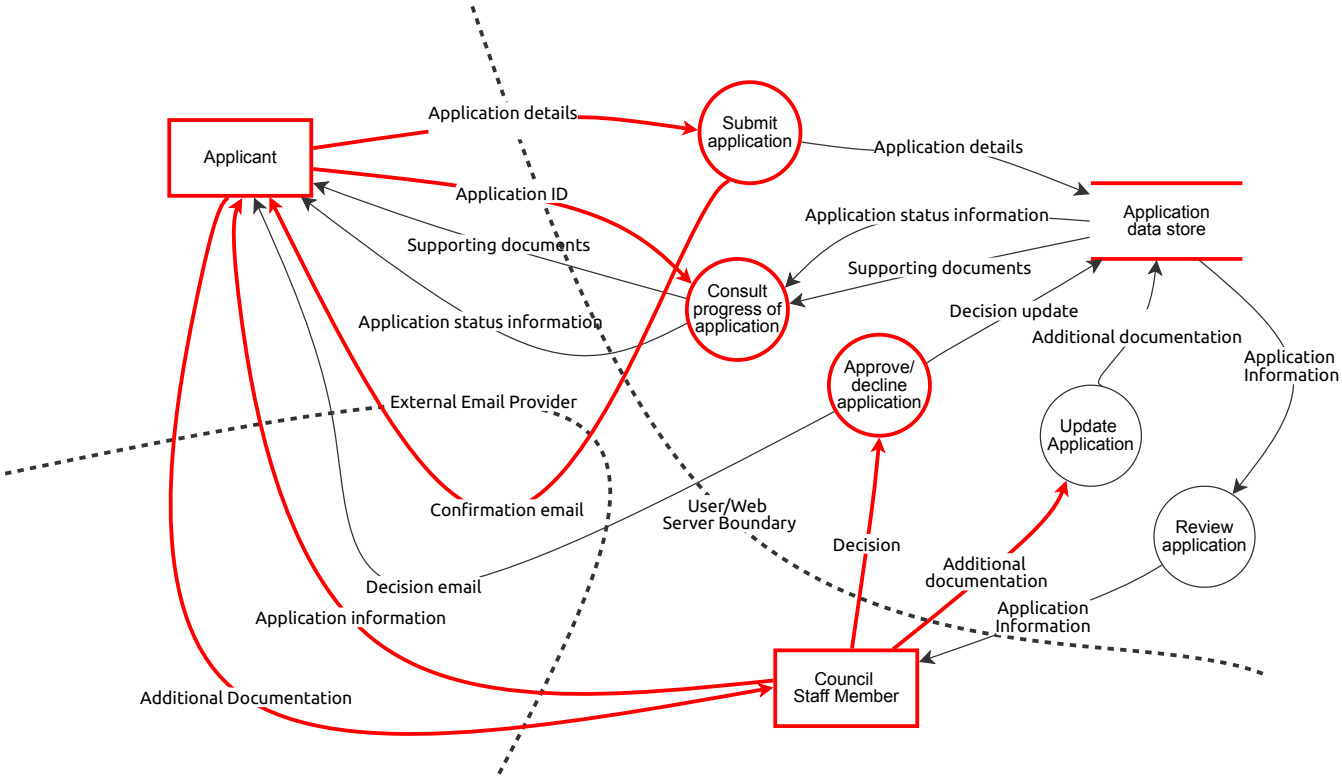
Number	Title	Type	Priority	Status	Score	Description	Mitigations
40	Session Hijacking	Spoofing	Medium	Mitigated		Staff session tokens get stolen by a threat actor and used maliciously to use the application as the staff member.	Use secure cookies with a session token sufficient length and entropy (128 bits long and at 64 bits of entropy). Also provide staff with training on avoiding phishing attacks and use email filters. This is also mitigated by all access to the system being behind a firewall

Number	Title	Type	Priority	Status	Score	Description	Mitigations
48	Repeated Requests	Denial of service	Medium	Mitigated		Repeated request attempts by an actor use significant resources such as CPU and memory	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, staff pages are behind a firewall and access is only allowed from the local council network or through a secure VPN. This prevents denial of service attacks from external actors.
51	Performing Actions Above Privilege Level	Elevation of privilege	Medium	Mitigated		By failing to restrict administration actions, staff members could perform actions above their privilege level.	Implement role based authorisation for all system actions.

Generic
Staff Action (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

main


Applicant
Application details
Submit application
Application details
Application data store
Application ID
Application status information
Supporting documents
Supporting documents
Consult progress of application
Application status information
Decision update
Additional documentation
Application Information
Approve/ decline application
External Email Provider
Update Application
Confirmation email
User/Web Server Boundary
Review application
Decision
Decision email
Additional documentation
Application information
Application Information
Additional Documentation
Council Staff Member

main

Applicant (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
121	Denying They Made an Application	Repudiation	Medium	Open		A user could deny they made an application	Log all actions taken by actors, including the actor's ip address, to ensure that the source of actions can be traced back to the actor that initiated them.
122	Email Account Stolen	Spoofing	Medium	Open		The applicant's email account could be stolen or hijacked, allowing a threat actor to act as the applicant.	Move all communication with the applicants to an authenticated web application. This would require applicants to create an account, then all communication is done over the application. The only information sent to the applicant via email would be telling them that they have a new message to view.
123	Applicant's Application ID Stolen	Spoofing	Medium	Open		If a threat actor discovered an application ID, they could view the applicant's supporting documents and find out information about their application.	

Council Staff Member (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
78	Impersonation of a Council Staff Member	Spoofing	Medium	Open		A threat actor could impersonate a council staff member and send emails to applicants requesting additional information (if they have their contact information through another means).	Purchase similar email domains to ensure threat actors can't use them. Use a simple email domain to make it easier for applicants to detect fake emails.
79	Session Hijacking	Spoofing	Medium	Open		Staff session tokens get stolen by a threat actor and used maliciously to use the application as the staff member.	Use secure cookies with a session token sufficient length and entropy (128 bits long and at 64 bits of entropy). Also provide staff with training on avoiding phishing attacks and use email filters.
80	Staff Credentials Stolen	Spoofing	Medium	Open		Staff credentials can be stolen via methods including brute force attacks, man in the middle attacks, them writing their details on a sticky note on their monitor, etc	Require two factor authentication and passwords that contain at least 10 characters, including at least one of each of upper case letter, lower case letter, number, and special character. Provide training to staff on best practices for password security.
81	Spoofed Account/Email Performing Malicious Actions	Repudiation	Medium	Mitigated		Accounts that have been spoofed can perform malicious acts without being able to prove whether the account was stolen by a threat actor.	Log all actions taken by actors, including login attempts with the actor's ip address, to ensure that the source of actions can be traced back to the actor that initiated them.

Submit application (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
88	Stealing Details with Fake Application Page	Spoofing	Medium	Open		A threat actor creates a fake application page resembling the real application page. This is then used to trick applicants into sharing their details with the threat actor.	Purchase similar domain names so that threat actors can't use them. Use a simple domain name so it's easier for the users to identify.
89	Repeated Applications	Denial of service	Medium	Open		Repeated applications by an actor use significant resources such as CPU and memory	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit.
90	Distributed Denial of Service Attack	Spoofing	Medium	Open		Similarly to the repeated login attempts, a distributed denial of service attack can cause significant CPU and memory usage. It can be hard to mitigate because requests come from lots of different sources, so can't all be blocked.	Use an access control list and scale up server capacity to allow for more concurrent requests. It is assumed that this is managed by the cloud service provider.
91	SQL/Code Injection	Elevation of privilege	Medium	Mitigated		When user inputs are not sanitised and handled correctly by the process, it can lead to malicious actions being performed within the process, leading the threat actor performing actions they don't have the privileges to do.	Sanitise user input so that it can't be executed as code.
92	Fake Applications	Repudiation	Medium	Mitigated		A threat actor could create fake applications to waste the council's time, then deny it.	Log all actions taken by actors with the actor's ip address, to ensure that the source of actions can be traced back to the actor that initiated them.

Review application (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Consult progress of application (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
97	Stealing Details with Fake Page	Spoofing	Medium	Open		A threat actor creates a fake page resembling the real page. This is then used to trick applicants into sharing their application ID with the threat actor.	Purchase similar domain names so that threat actors can't use them. Use a simple domain name so it's easier for the users to identify.
98	Repeated Requests	Denial of service	Medium	Open		Repeated requests by an actor use significant resources such as CPU and memory	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit.
99	Distributed Denial of Service Attack	Denial of service	Medium	Open		Similarly to the repeated login attempts, a distributed denial of service attack can cause significant CPU and memory usage. It can be hard to mitigate because requests come from lots of different sources, so can't all be blocked.	Use an access control list and scale up server capacity to allow for more concurrent requests. It is assumed that this is managed by the cloud service provider.
100	SQL/Code Injection	Elevation of privilege	Medium	Mitigated		When user inputs are not sanitised and handled correctly by the process, it can lead to malicious actions being performed within the process, leading the threat actor performing actions they don't have the privileges to do.	Sanitise user input so that it can't be executed as code.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
101	Spam Requests	Repudiation	Medium	Mitigated		A threat actor could request documents to waste the council's time, then deny it.	Log all actions taken by actors with the actor's ip address, to ensure that the source of actions can be traced back to the actor that initiated them.
102	Actor Requesting Information on Another Application	Information disclosure	Medium	Open		An applicant could request information for another application if they had the application ID. This could be guessed since they're only 8 characters	Make application ID's random rather then sequential. It could be further reduced by using a longer application ID, such as 16 characters, or preferably, implementing a login system for applications.

Approve/ decline application (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
107	Fake Emails	Spoofing	Medium	Open		A threat actor could send out emails to applicants saying that their application has been approved or declined (if they have their contact information through another means).	Purchase similar email domains to ensure threat actors can't use them. Use a simple email domain to make it easier for applicants to detect fake emails.
109	False Claim of Application Approval	Repudiation	Medium	Mitigated		An applicant could claim their application has been approved, when it hasn't. This may be due to a spoofed or tampered email, or general dishonesty.	Log and save all application status changes.
110	Information Sent to the Wrong Applicant	Information disclosure	Medium	Open		An application status update could be sent to the wrong applicant. This would disclose information about the intended recipient, and their decision number.	Move all communication with the applicants to an authenticated web application. This would require applicants to create an account, then all communication is done over the application. The only information sent to the applicant via email would be telling them that they have a new message to view.

Application data store (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
58	Database Filling Up	Denial of service	Medium	Open		If the system receives significantly more applications than expected, the database could run out of space to store information about new applications.	Partially mitigate by enabling storage notifications to system administrators so that they can increase the size of the database.

Application Information (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Additional documentation (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Application status information (Data Flow)

Status
Staff member responsible
Supporting documents (optional)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Decision update (Data Flow)

Status and decision number

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Application details (Data Flow)

All application details plus the 8-digit application identifier

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Supporting documents (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Supporting documents (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
61	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the user, gaining access to the supporting documents	Require HTTPS and transport layer security.

Application status information (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
70	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the user, gaining access to their application information	Require HTTPS and transport layer security.

Decision (Data Flow)

Decision number and decision status

Number	Title	Type	Priority	Status	Score	Description	Mitigations
82	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the system, modify the intended action, then forward it to the system.	Require HTTPS and transport layer security.
83	Repeated Requests	Denial of service	Medium	Open		A malicious actor repeatedly sends requests to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, you could put staff pages behind a firewall and only allow access from the local council network or through a secure VPN. However, this is not feasible in the current system as there is a requirement for the website to be publicly available.

Additional documentation (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
84	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the system, modify the intended action or steal data, then forward it to the system.	Require HTTPS and transport layer security.
85	Repeated Requests	Denial of service	Medium	Open		A malicious actor repeatedly sends requests to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Additionally, you could put staff pages behind a firewall and only allow access from the local council network or through a secure VPN. However, this is not feasible in the current system as there is a requirement for the website to be publicly available.

Application Information (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
87	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the staff member.	Require HTTPS and transport layer security.

Application details

(Data Flow)

For each property owner:
- pronoun
- first name
- last name
- email
- phone number

Details of the property (just its address)
And supporting documents

Number	Title	Type	Priority	Status	Score	Description	Mitigations
57	Repeated Applications	Denial of service	Medium	Open		A malicious actor repeatedly sends applications to the system, slowing down access for other actors	As a simple mitigation, limit the number of applications from a single phone number or email address in a certain time frame. Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit.
59	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the system, modify the data, then forward it to the system. They could also intercept the applicant's personal information and supporting documents, and use them for their personal gain.	Require HTTPS and transport layer security.

Application ID (Data Flow)

Also maybe a supporting documentation flag?

Number	Title	Type	Priority	Status	Score	Description	Mitigations
62	Brute Force Attack	Information disclosure	Medium	Open		Given the application ID is only 8 characters, a threat actor could obtain it via brute force methods. This could lead to supporting documents being accessible to the threat actor.	Rate limiting and logging could partially mitigate this threat. It could be further reduced by using a longer application ID, such as 16 characters, or preferably, implementing a login system for applications.
63	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor intercepts the application ID submitted to the application.	Require HTTPS and transport layer security.
67	Repeated Requests	Denial of service	Medium	Open		A malicious actor repeatedly sends requests to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit.

Additional Documentation (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
75	Adversary in the Middle Attack	Tampering	Medium	Open		A threat actor can intercept emails from the applicant to the council. This would allow them to gain access to the additional documentation about the application the applicant is sending.	Use an email provider with encryption and that can only be accessed through HTTPS
77	Repeated Emails	Denial of service	Medium	Mitigated		A threat actor could send repeated emails to the council system, overwhelming the server.	It is assumed that this is handled by the email server.

Application information (Data Flow)

Summary of application and the extra information to be provided

Number	Title	Type	Priority	Status	Score	Description	Mitigations
74	Adversary in the Middle Attack	Tampering	Medium	Open		A threat actor can intercept emails meant for the user, gaining access to information about their application	Use an email provider with encryption and that can only be accessed through HTTPS

Decision email (Data Flow)

Email with decision number and a letter of confirmation/denial.
Sent to all relevant applicants

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Confirmation email (Data Flow)

Email with 8-digit application code
confirming application.
Also includes summary of the application.

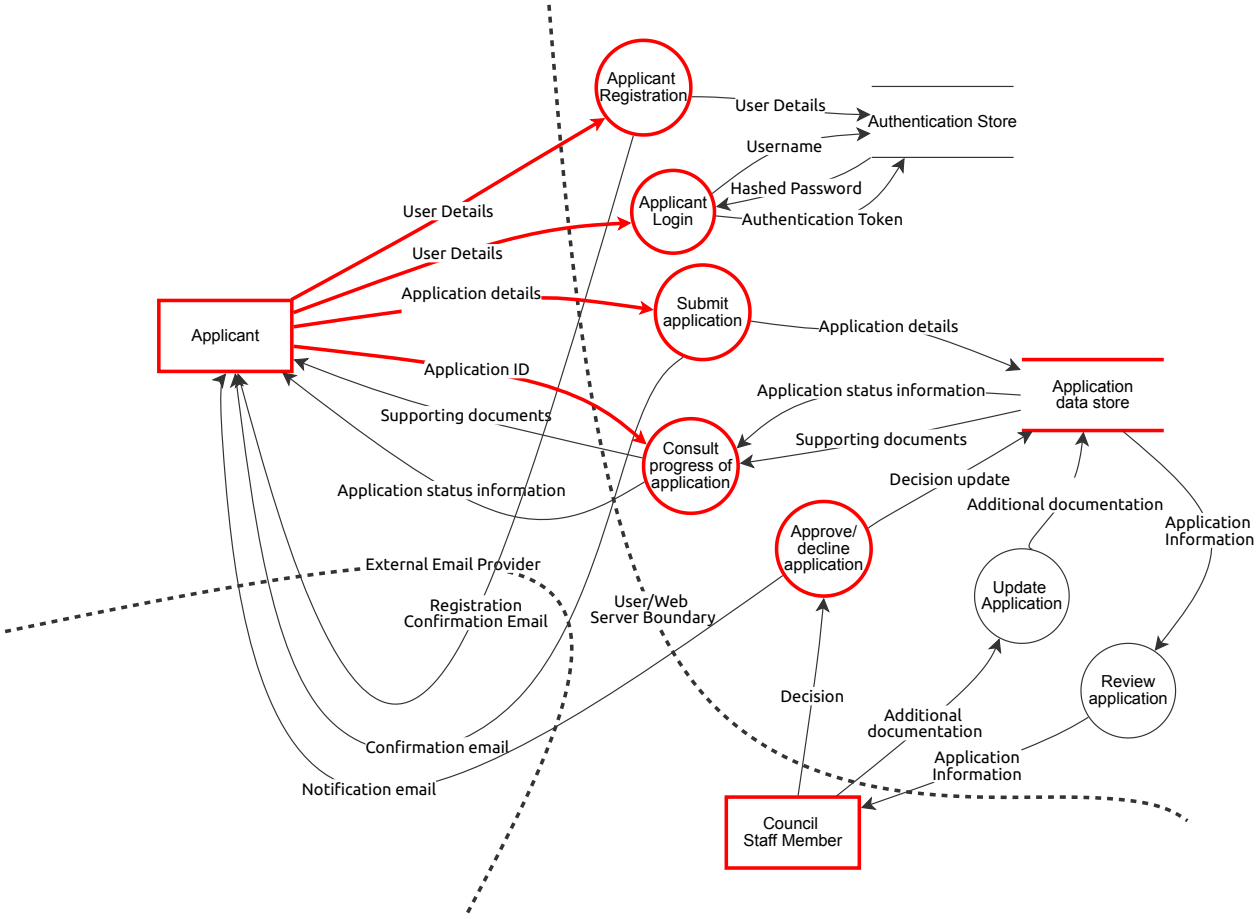
Number	Title	Type	Priority	Status	Score	Description	Mitigations
71	Adversary in the Middle Attack	Tampering	Medium	Open		A threat actor can intercept emails meant for the user, gaining access to their application ID, and therefore their supporting documents.	Use an email provider with encryption and that can only be accessed through HTTPS

Update Application (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
117	SQL/Code Injection	Elevation of privilege	Medium	Mitigated		If user input isn't sanitised or handled properly, a threat actor could use this to perform malicious actions, such as editing an application they shouldn't be, or deleting applications.	Sanitise user input so that it can't be executed as code.

main - authenticated applicants

An updated version of the main diagram where applicants must create an account rather than just using the application ID to access everything



main - authenticated applicants

Applicant (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
121	Denying They Made an Application	Repudiation	Medium	Open		A user could deny they made an application	Log all actions taken by actors, including the actor's ip address, to ensure that the source of actions can be traced back to the actor that initiated them.
122	Email Account Stolen	Spoofing	Medium	Open		The applicant's email account could be stolen or hijacked, allowing a threat actor to act as the applicant.	Move all communication with the applicants to an authenticated web application. This would require applicants to create an account, then all communication is done over the application. The only information sent to the applicant via email would be telling them that they have a new message to view.
123	Applicant's Application ID Stolen	Spoofing	Medium	Open		If a threat actor discovered an application ID, they could view the applicant's supporting documents and find out information about their application.	

Council Staff Member (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
78	Impersonation of a Council Staff Member	Spoofing	Medium	Open		A threat actor could impersonate a council staff member and send emails to applicants requesting additional information (if they have their contact information through another means).	Purchase similar email domains to ensure threat actors can't use them. Use a simple email domain to make it easier for applicants to detect fake emails.
79	Session Hijacking	Spoofing	Medium	Open		Staff session tokens get stolen by a threat actor and used maliciously to use the application as the staff member.	Use secure cookies with a session token sufficient length and entropy (128 bits long and at 64 bits of entropy). Also provide staff with training on avoiding phishing attacks and use email filters.
80	Staff Credentials Stolen	Spoofing	Medium	Open		Staff credentials can be stolen via methods including brute force attacks, man in the middle attacks, them writing their details on a sticky note on their monitor, etc	Require two factor authentication and passwords that contain at least 10 characters, including at least one of each of upper case letter, lower case letter, number, and special character. Provide training to staff on best practices for password security.
81	Spoofed Account/Email Performing Malicious Actions	Repudiation	Medium	Mitigated		Accounts that have been spoofed can perform malicious acts without being able to prove whether the account was stolen by a threat actor.	Log all actions taken by actors, including login attempts with the actor's ip address, to ensure that the source of actions can be traced back to the actor that initiated them.

Submit application (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
88	Stealing Details with Fake Application Page	Spoofing	Medium	Open		A threat actor creates a fake application page resembling the real application page. This is then used to trick applicants into sharing their details with the threat actor.	Purchase similar domain names so that threat actors can't use them. Use a simple domain name so it's easier for the users to identify.
89	Repeated Applications	Denial of service	Medium	Open		Repeated applications by an actor use significant resources such as CPU and memory	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit.
90	Distributed Denial of Service Attack	Spoofing	Medium	Open		Similarly to the repeated login attempts, a distributed denial of service attack can cause significant CPU and memory usage. It can be hard to mitigate because requests come from lots of different sources, so can't all be blocked.	Use an access control list and scale up server capacity to allow for more concurrent requests. It is assumed that this is managed by the cloud service provider.
91	SQL/Code Injection	Elevation of privilege	Medium	Mitigated		When user inputs are not sanitised and handled correctly by the process, it can lead to malicious actions being performed within the process, leading the threat actor performing actions they don't have the privileges to do.	Sanitise user input so that it can't be executed as code.
92	Fake Applications	Repudiation	Medium	Mitigated		A threat actor could create fake applications to waste the council's time, then deny it.	Log all actions taken by actors with the actor's ip address, to ensure that the source of actions can be traced back to the actor that initiated them.

Review application (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Consult progress of application (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
97	Stealing Details with Fake Page	Spoofing	Medium	Open		A threat actor creates a fake page resembling the real page. This is then used to trick applicants into sharing their application ID with the threat actor.	Purchase similar domain names so that threat actors can't use them. Use a simple domain name so it's easier for the users to identify.
98	Repeated Requests	Denial of service	Medium	Open		Repeated requests by an actor use significant resources such as CPU and memory	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit.
99	Distributed Denial of Service Attack	Denial of service	Medium	Open		Similarly to the repeated login attempts, a distributed denial of service attack can cause significant CPU and memory usage. It can be hard to mitigate because requests come from lots of different sources, so can't all be blocked.	Use an access control list and scale up server capacity to allow for more concurrent requests. It is assumed that this is managed by the cloud service provider.
100	SQL/Code Injection	Elevation of privilege	Medium	Mitigated		When user inputs are not sanitised and handled correctly by the process, it can lead to malicious actions being performed within the process, leading the threat actor performing actions they don't have the privileges to do.	Sanitise user input so that it can't be executed as code.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
101	Spam Requests	Repudiation	Medium	Mitigated		A threat actor could request documents to waste the council's time, then deny it.	Log all actions taken by actors with the actor's ip address, to ensure that the source of actions can be traced back to the actor that initiated them.
102	Actor Requesting Information on Another Application	Information disclosure	Medium	Open		An applicant could request information for another application if they had the application ID. This could be guessed since they're only 8 characters	Make application ID's random rather then sequential. It could be further reduced by using a longer application ID, such as 16 characters, or preferably, implementing a login system for applications.

Approve/ decline application (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
107	Fake Emails	Spoofing	Medium	Open		A threat actor could send out emails to applicants saying that their application has been approved or declined (if they have their contact information through another means).	Purchase similar email domains to ensure threat actors can't use them. Use a simple email domain to make it easier for applicants to detect fake emails.
109	False Claim of Application Approval	Repudiation	Medium	Mitigated		An applicant could claim their application has been approved, when it hasn't. This may be due to a spoofed or tampered email, or general dishonesty.	Log and save all application status changes.
110	Information Sent to the Wrong Applicant	Information disclosure	Medium	Open		An application status update could be sent to the wrong applicant. This would disclose information about the intended recipient, and their decision number.	Move all communication with the applicants to an authenticated web application. This would require applicants to create an account, then all communication is done over the application. The only information sent to the applicant via email would be telling them that they have a new message to view.

Application data store (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
58	Database Filling Up	Denial of service	Medium	Open		If the system receives significantly more applications than expected, the database could run out of space to store information about new applications.	Partially mitigate by enabling storage notifications to system administrators so that they can increase the size of the database.

Application Information (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Additional documentation (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Application status information (Data Flow)

Status
Staff member responsible
Supporting documents (optional)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Decision update (Data Flow)

Status and decision number

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Application details (Data Flow)

All application details plus the 8-digit application identifier

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Supporting documents (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Supporting documents (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
61	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the user, gaining access to the supporting documents	Require HTTPS and transport layer security.

Application status information (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
70	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the user, gaining access to their application information	Require HTTPS and transport layer security.

Confirmation email (Data Flow)

Email with 8-digit application code confirming application.
Also includes summary of the application.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
71	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept emails meant for the user, gaining access to their application ID, and therefore their supporting documents.	Use an email provider with encryption and that can only be accessed through HTTPS

Application Information (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
87	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the staff member.	Require HTTPS and transport layer security.

Hashed Password (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Hashed Password (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authentication Token (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

User Details (Data Flow)

Email, password, phone number

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Registration Confirmation Email (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Notification email (Data Flow)

An email telling the user that they have a new message about their application - Notably does not include a link to view the message

Number	Title	Type	Priority	Status	Score	Description	Mitigations
74	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept emails meant for the user, gaining access to information about their application	Use an email provider with encryption and that can only be accessed through HTTPS

Application details (Data Flow)

For each property owner:
- pronoun
- first name
- last name
- email
- phone number

Details of the property (just its address)
And supporting documents

Number	Title	Type	Priority	Status	Score	Description	Mitigations
57	Repeated Applications	Denial of service	Medium	Open		A malicious actor repeatedly sends applications to the system, slowing down access for other actors	As a simple mitigation, limit the number of applications from a single phone number or email address in a certain time frame. Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit.
59	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the system, modify the data, then forward it to the system. They could also intercept the applicant's personal information and supporting documents, and use them for their personal gain.	Require HTTPS and transport layer security.

User Details (Data Flow)

Email, password, phone number

Number	Title	Type	Priority	Status	Score	Description	Mitigations
151	Repeated Registration	Denial of service	Medium	Open		A malicious actor repeatedly sends registrations to the system, slowing down access for other actors	As a simple mitigation, limit the number of applications from a single phone number or email address in a certain time frame. Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit.
154	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the system, modify the data, then forward it to the system. They could also intercept the applicant's personal information and supporting documents, and use them for their personal gain.	Require HTTPS and transport layer security.

User Details (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
155	Repeated Applications	Denial of service	Medium	Open		A malicious actor repeatedly sends applications to the system, slowing down access for other actors	As a simple mitigation, limit the number of applications from a single phone number or email address in a certain time frame. Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit.
156	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the system, modify the data, then forward it to the system. They could also intercept the applicant's personal information and supporting documents, and use them for their personal gain.	Require HTTPS and transport layer security.

Decision (Data Flow)

Decision number and decision status

Number	Title	Type	Priority	Status	Score	Description	Mitigations
82	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the system, modify the intended action, then forward it to the system.	Require HTTPS and transport layer security.
83	Repeated Requests	Denial of service	Medium	Mitigated		A malicious actor repeatedly sends requests to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Placed staff pages behind a firewall and only allowed access from the local council network or through a secure VPN. (see login diagram for information on the firewall)

Additional documentation (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
84	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor can intercept packets meant for the system, modify the intended action or steal data, then forward it to the system.	Require HTTPS and transport layer security.
85	Repeated Requests	Denial of service	Medium	Mitigated		A malicious actor repeatedly sends requests to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit. Placed staff pages behind a firewall and only allowed access from the local council network or through a secure VPN. (see login diagram for information on the firewall)

Application ID (Data Flow)

Also maybe a supporting documentation flag?

Number	Title	Type	Priority	Status	Score	Description	Mitigations
62	Brute Force Attack	Information disclosure	Medium	Mitigated		Given the application ID is only 8 characters, a threat actor could obtain it via brute force methods. This could lead to supporting documents being accessible to the threat actor.	Mitigated by implementing a login system for applications. This completely removes the threat.
63	Adversary in the Middle Attack	Tampering	Medium	Mitigated		A threat actor intercepts the application ID submitted to the application.	Require HTTPS and transport layer security.
67	Repeated Requests	Denial of service	Medium	Open		A malicious actor repeatedly sends requests to the system, slowing down access for other actors	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit.

Update Application (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
117	SQL/Code Injection	Elevation of privilege	Medium	Mitigated		If user input isn't sanitised or handled properly, a threat actor could use this to perform malicious actions, such as editing an application they shouldn't be, or deleting applications.	Sanitise user input so that it can't be executed as code.

Applicant Login (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
160	Stealing Credentials with Fake Login Page	Spoofing	Medium	Open		A threat actor creates a fake login page resembling the real login page. This is then used to trick users into sharing their login details with the threat actor.	Purchase similar domain names so that threat actors can't use them. Use a simple domain name so it's easier for the users to identify.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
161	Disclosure of Used Usernames	Information disclosure	Medium	Mitigated		When the actor supplies an incorrect or invalid username or password, they can determine whether the username is used in the system because the feedback specifies which field is invalid.	Only provide generic feedback stating that the username or password is incorrect.
162	Repeated Login Attempts	Denial of service	Medium	Open		Repeated login attempts by an actor use significant resources such as CPU and memory	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit.
163	SQL/Code Injection	Spoofing	Medium	Mitigated		When user inputs are not sanitised and handled correctly by the process, it can lead to malicious actions being performed within the process, leading the threat actor performing actions they don't have the privileges to do.	Sanitise user input so that it can't be executed as code.

Applicant Registration (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
157	Stealing Credentials with Fake Registration Page	Spoofing	Medium	Open		A threat actor creates a fake registration page resembling the real login page. This is then used to trick users into sharing their details with the threat actor.	Purchase similar domain names so that threat actors can't use them. Use a simple domain name so it's easier for the users to identify.
158	Repeated Registration Attempts	Denial of service	Medium	Open		Repeated registration attempts by an actor use significant resources such as CPU and memory	Put a limit on the number of requests allowed from a single IP address within a certain time frame. Blacklist users who repeatedly exceed this limit.
159	SQL/Code Injection	Elevation of privilege	Medium	Open		When user inputs are not sanitised and handled correctly by the process, it can lead to malicious actions being performed within the process, leading the threat actor performing actions they don't have the privileges to do.	Sanitise user input so that it can't be executed as code.

Authentication Store (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
164	Data Tampering	Tampering	Medium	Mitigated		An actor gains access to the authentication store and alters or removes entries	Store database credentials in a secure location and not in plain text. Store user credentials in an encrypted form. Again use the least privileged principle. Also only allow read access to the database from the login endpoint.
165	Visibility of Restricted Data	Tampering	Medium	Mitigated		Users should not be able to see information about other actors credentials.	Apply the least privileged principle to ensure the minimum required amount data is visible.