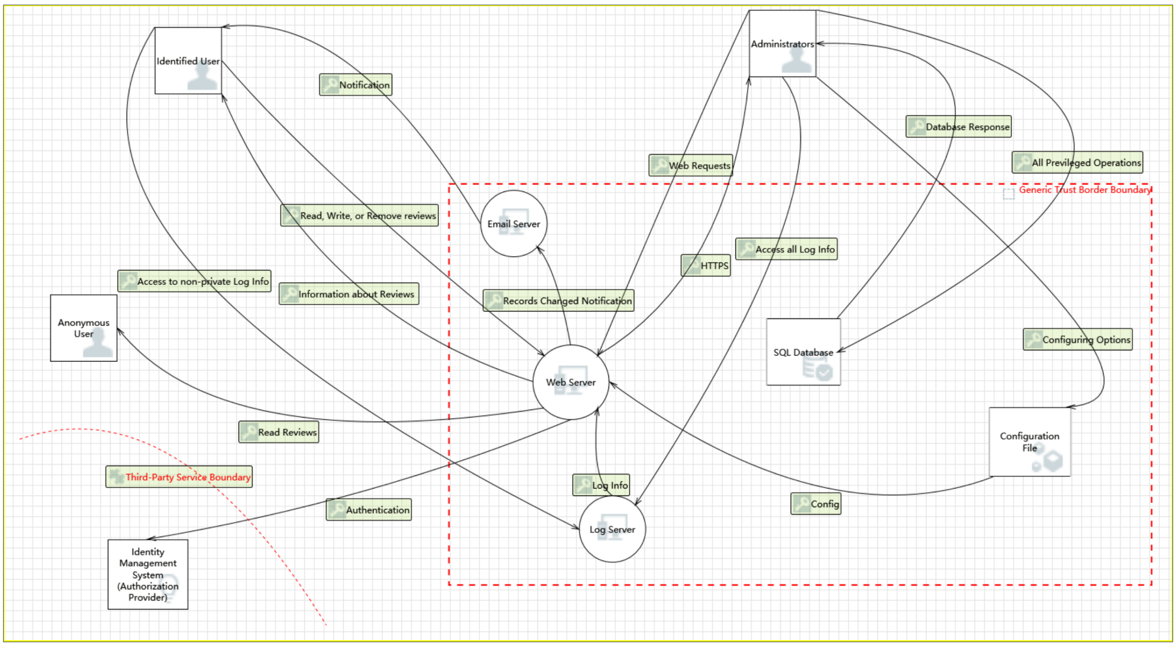
CS 542 – Introduction to Software Security
Exercise on Threat Modeling

Binhao Chen (bchen276@wisc.edu), Steven Yang (yang558@wisc.edu)

Due: November 15 at 2:30pm

1 The diagram modeling the system.

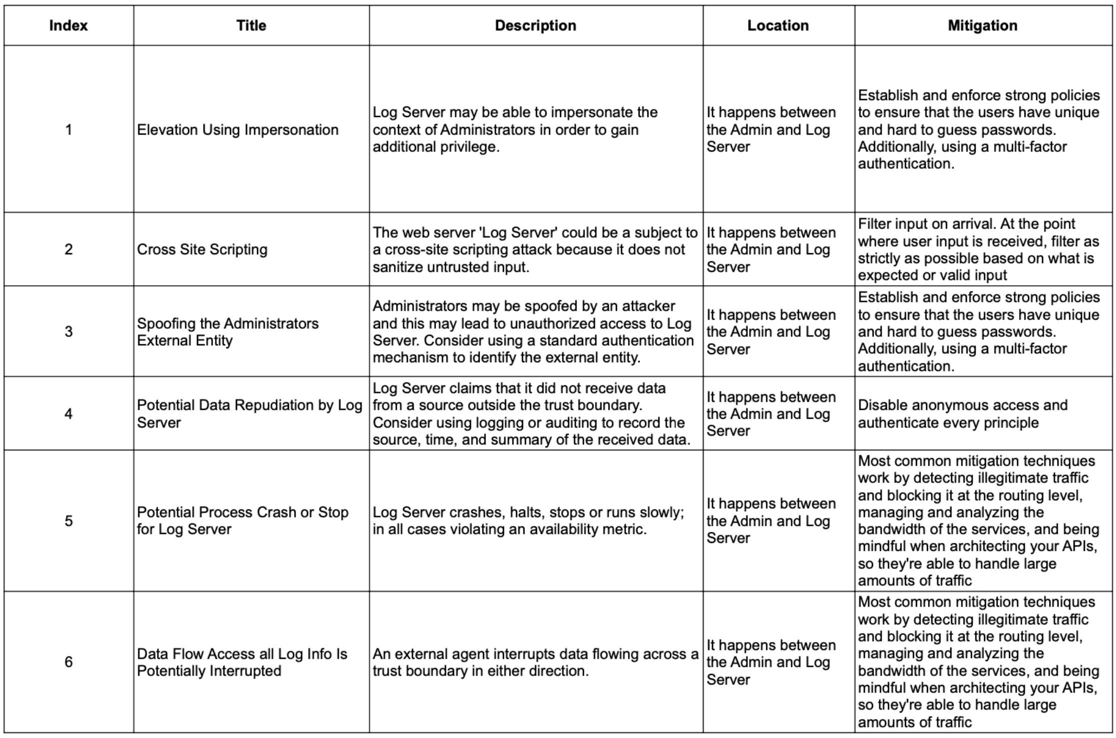
Diagram: Diagram 1

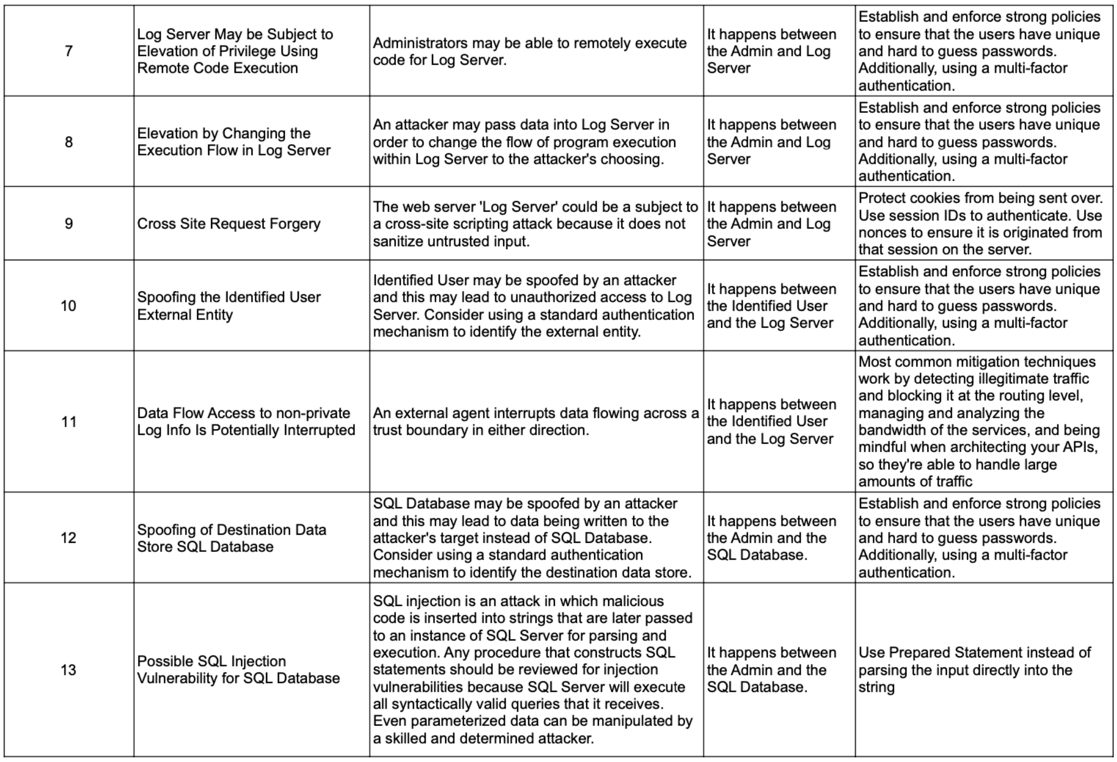

Identified User
Notification
Administrators
Database Response
All Previleged Operations
Web Requests
Generic Trust Border Boundary
Email Server
Read, Write, or Remove reviews
Access all Log Info
HTTPS
Access to non-private Log Info
Information about Reviews
Records Changed Notification
Anonymous User
SQL Database
Configuring Options
Web Server
Configuration File
Read Reviews
Third-Party Service Boundary
Log Info
Config
Authentication
Log Server
Identity Management System (Authorization Provider)

2 The number of threats found by the tool

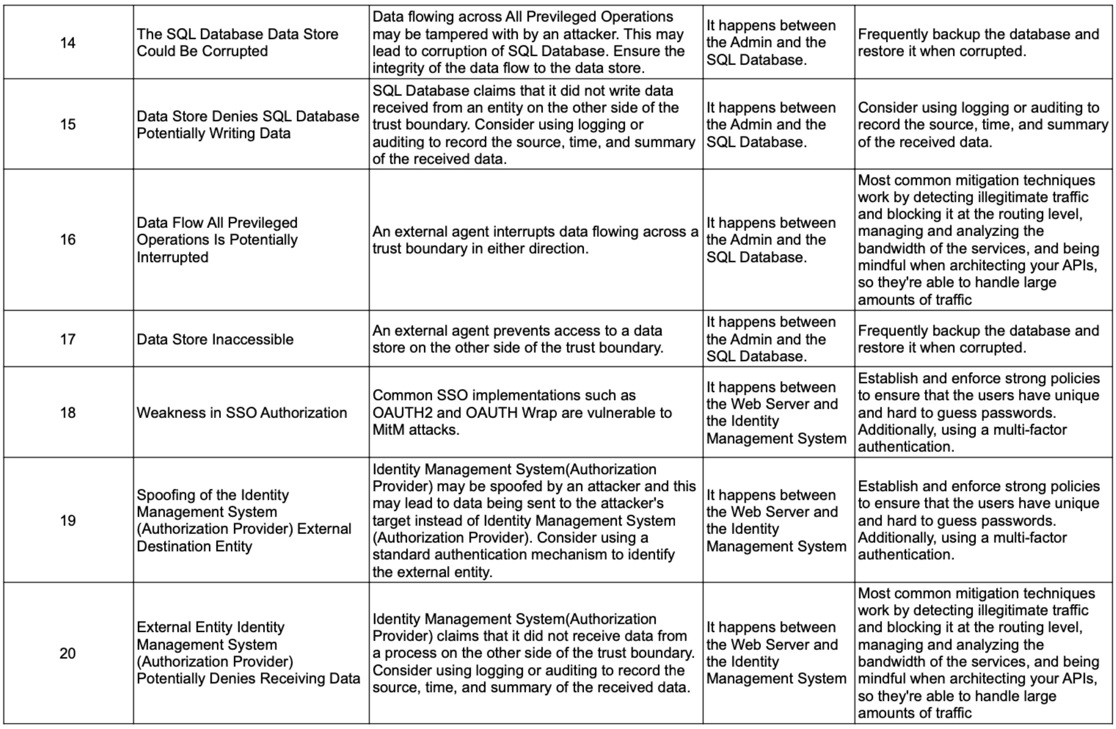
In total, our model has 76 threats found by the tool.

3 A table containing an entry for each different threat, and an example of where that threat happens in your design, and what would you do to mitigate it.

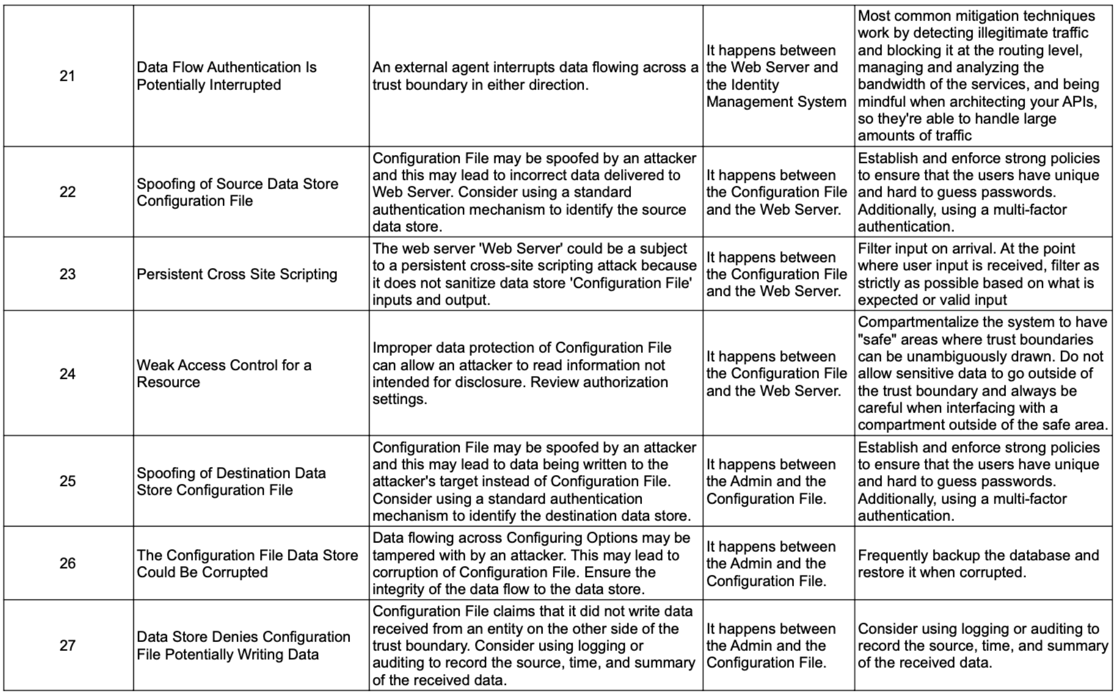




Index	Title	Description	Location	Mitigation
1	Elevation Using Impersonation	Log Server may be able to impersonate the context of Administrators in order to gain additional privilege.	It happens between the Admin and Log Server	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
2	Cross Site Scripting	The web server 'Log Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.	It happens between the Admin and Log Server	Filter input on arrival. At the point where user input is received, filter as strictly as possible based on what is expected or valid input
3	Spoofing the Administrators External Entity	Administrators may be spoofed by an attacker and this may lead to unauthorized access to Log Server. Consider using a standard authentication mechanism to identify the external entity.	It happens between the Admin and Log Server	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
4	Potential Data Repudiation by Log Server	Log Server claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	It happens between the Admin and Log Server	Disable anonymous access and authenticate every principle
5	Potential Process Crash or Stop for Log Server	Log Server crashes, halts, stops or runs slowly; in all cases violating an availability metric.	It happens between the Admin and Log Server	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
6	Data Flow Access all Log Info Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	It happens between the Admin and Log Server	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
7	Log Server May be Subject to Elevation of Privilege Using Remote Code Execution	Administrators may be able to remotely execute code for Log Server.	It happens between the Admin and Log Server	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
8	Elevation by Changing the Execution Flow in Log Server	An attacker may pass data into Log Server in order to change the flow of program execution within Log Server to the attacker's choosing.	It happens between the Admin and Log Server	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
9	Cross Site Request Forgery	The web server 'Log Server' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.	It happens between the Admin and Log Server	Protect cookies from being sent over. Use session IDs to authenticate. Use nonces to ensure it is originated from that session on the server.
10	Spoofing the Identified User External Entity	Identified User may be spoofed by an attacker and this may lead to unauthorized access to Log Server. Consider using a standard authentication mechanism to identify the external entity.	It happens between the Identified User and the Log Server	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
11	Data Flow Access to non-private Log Info Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	It happens between the Identified User and the Log Server	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
12	Spoofing of Destination Data Store SQL Database	SQL Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of SQL Database. Consider using a standard authentication mechanism to identify the destination data store.	It happens between the Admin and the SQL Database.	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
13	Possible SQL Injection Vulnerability for SQL Database	SQL injection is an attack in which malicious code is inserted into strings that are later passed to an instance of SQL Server for parsing and execution. Any procedure that constructs SQL statements should be reviewed for injection vulnerabilities because SQL Server will execute all syntactically valid queries that it receives. Even parameterized data can be manipulated by a skilled and determined attacker.	It happens between the Admin and the SQL Database.	Use Prepared Statement instead of parsing the input directly into the string

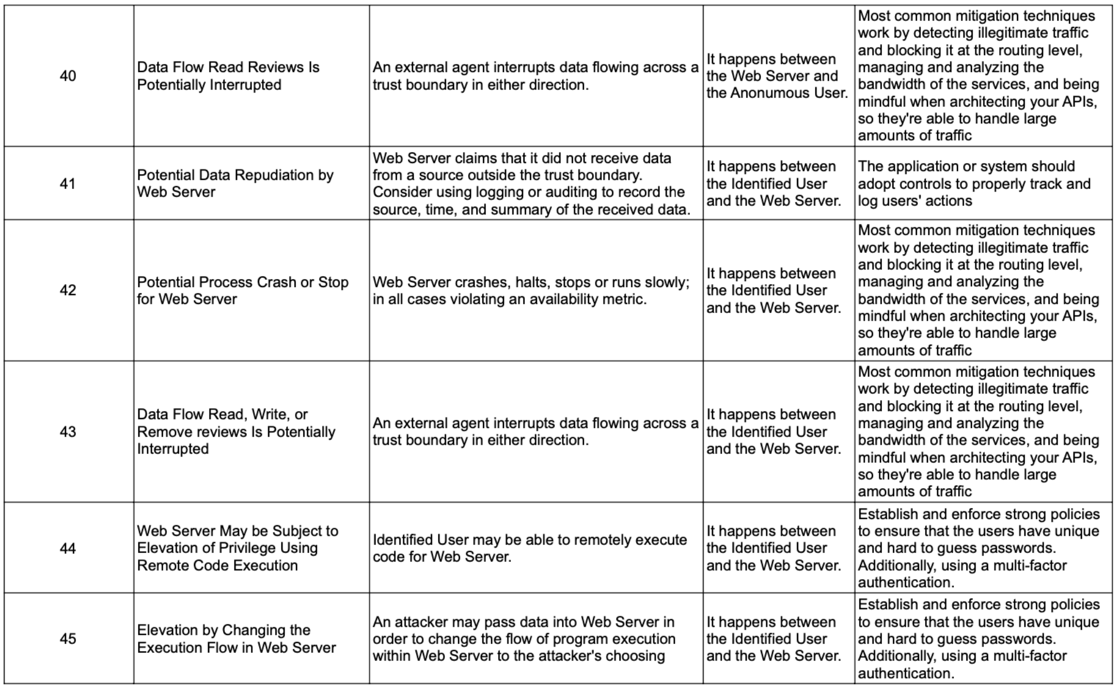


14	The SQL Database Data Store Could Be Corrupted	Data flowing across All Previleged Operations may be tampered with by an attacker. This may lead to corruption of SQL Database. Ensure the integrity of the data flow to the data store.	It happens between the Admin and the SQL Database.	Frequently backup the database and restore it when corrupted.
15	Data Store Denies SQL Database Potentially Writing Data	SQL Database claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	It happens between the Admin and the SQL Database.	Consider using logging or auditing to record the source, time, and summary of the received data.
16	Data Flow All Previleged Operations Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	It happens between the Admin and the SQL Database.	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
17	Data Store Inaccessible	An external agent prevents access to a data store on the other side of the trust boundary.	It happens between the Admin and the SQL Database.	Frequently backup the database and restore it when corrupted.
18	Weakness in SSO Authorization	Common SSO implementations such as OAUTH2 and OAUTH Wrap are vulnerable to MitM attacks.	It happens between the Web Server and the Identity Management System	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
19	Spoofing of the Identity Management System (Authorization Provider) External Destination Entity	Identity Management System(Authorization Provider) may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Identity Management System (Authorization Provider). Consider using a standard authentication mechanism to identify the external entity.	It happens between the Web Server and the Identity Management System	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
20	External Entity Identity Management System (Authorization Provider) Potentially Denies Receiving Data	Identity Management System(Authorization Provider) claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	It happens between the Web Server and the Identity Management System	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic

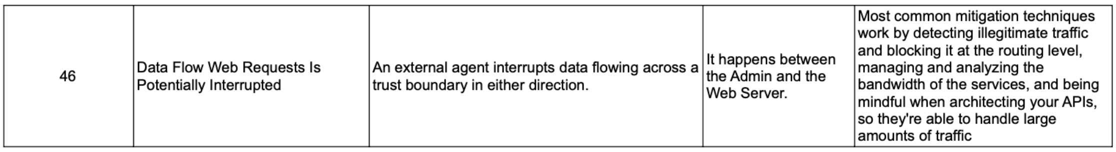


21	Data Flow Authentication Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	It happens between the Web Server and the Identity Management System	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
22	Spoofing of Source Data Store Configuration File	Configuration File may be spoofed by an attacker and this may lead to incorrect data delivered to Web Server. Consider using a standard authentication mechanism to identify the source data store.	It happens between the Configuration File and the Web Server.	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
23	Persistent Cross Site Scripting	The web server 'Web Server' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'Configuration File' inputs and output.	It happens between the Configuration File and the Web Server.	Filter input on arrival. At the point where user input is received, filter as strictly as possible based on what is expected or valid input
24	Weak Access Control for a Resource	Improper data protection of Configuration File can allow an attacker to read information not intended for disclosure. Review authorization settings.	It happens between the Configuration File and the Web Server.	Compartmentalize the system to have "safe" areas where trust boundaries can be unambiguously drawn. Do not allow sensitive data to go outside of the trust boundary and always be careful when interfacing with a compartment outside of the safe area.
25	Spoofing of Destination Data Store Configuration File	Configuration File may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of Configuration File. Consider using a standard authentication mechanism to identify the destination data store.	It happens between the Admin and the Configuration File.	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
26	The Configuration File Data Store Could Be Corrupted	Data flowing across Configuring Options may be tampered with by an attacker. This may lead to corruption of Configuration File. Ensure the integrity of the data flow to the data store.	It happens between the Admin and the Configuration File.	Frequently backup the database and restore it when corrupted.
27	Data Store Denies Configuration File Potentially Writing Data	Configuration File claims that it did not write data received from an entity on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	It happens between the Admin and the Configuration File.	Consider using logging or auditing to record the source, time, and summary of the received data.

28	Data Flow Configuring Options Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	It happens between the Admin and the Configuration File.	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
29	Spoofing of Source Data Store SQL Database	SQL Database may be spoofed by an attacker and this may lead to incorrect data delivered to Administrators. Consider using a standard authentication mechanism to identify the source data store.	It happens between the SQL Database and the Admin.	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
30	External Entity Administrators Potentially Denies Receiving Data	Administrators claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	It happens between the SQL Database and the Admin.	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
31	Data Flow Database Response Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	It happens between the SQL Database and the Admin.	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
32	Spoofing of the Administrators External Destination Entity	Administrators may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Administrators. Consider using a standard authentication mechanism to identify the external entity.	It happens between the Web Server and the Admin.	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
33	Data Flow HTTPS Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	It happens between the Web Server and the Admin.	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
34	Spoofing of the Identified User External Destination Entity	Identified User may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Identified User. Consider using a standard authentication mechanism to identify the external entity.	It happens between the Web Server and the Identified User.	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
35	External Entity Identified User Potentially Denies Receiving Data	Identified User claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	It happens between the Web Server and the Identified User.	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
36	Data Flow Information about Reviews Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	It happens between the Web Server and the Identified User.	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
37	Data Flow Notification Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	It happens between Email Server and the Identified User.	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
38	Spoofing of the Anonymous User External Destination Entity	Anonymous User may be spoofed by an attacker and this may lead to data being sent to the attacker's target instead of Anonymous User. Consider using a standard authentication mechanism to identify the external entity.	It happens between Email Server and the Identified User.	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
39	External Entity Anonymous User Potentially Denies Receiving Data	Anonymous User claims that it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	It happens between the Web Server and the Anonumous User.	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic



40	Data Flow Read Reviews Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	It happens between the Web Server and the Anonumous User.	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
41	Potential Data Repudiation by Web Server	Web Server claims that it did not receive data from a source outside the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.	It happens between the Identified User and the Web Server.	The application or system should adopt controls to properly track and log users' actions
42	Potential Process Crash or Stop for Web Server	Web Server crashes, halts, stops or runs slowly; in all cases violating an availability metric.	It happens between the Identified User and the Web Server.	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
43	Data Flow Read, Write, or Remove reviews Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	It happens between the Identified User and the Web Server.	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic
44	Web Server May be Subject to Elevation of Privilege Using Remote Code Execution	Identified User may be able to remotely execute code for Web Server.	It happens between the Identified User and the Web Server.	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.
45	Elevation by Changing the Execution Flow in Web Server	An attacker may pass data into Web Server in order to change the flow of program execution within Web Server to the attacker's choosing	It happens between the Identified User and the Web Server.	Establish and enforce strong policies to ensure that the users have unique and hard to guess passwords. Additionally, using a multi-factor authentication.



46	Data Flow Web Requests Is Potentially Interrupted	An external agent interrupts data flowing across a trust boundary in either direction.	It happens between the Admin and the Web Server.	Most common mitigation techniques work by detecting illegitimate traffic and blocking it at the routing level, managing and analyzing the bandwidth of the services, and being mindful when architecting your APIs, so they're able to handle large amounts of traffic

4 What are the weakest points of your design?

The weakest points of our design are:
1. Data Flow Potentially Interrupted exists between several system components.
2. Elevation of Privilege Using Remote Code Execution is also worth noting.
3. It may be vulnerable to spoofing of the Administrators Entity to perform malicious actions.

5 Should you re-design part of your system?

Yes. Since there are lots of threats happen between Admin and the SQL Database, and there are also issues with spoofing the Admin identity, we could add one more authentication when the Admin is trying to interact with the SQL Database in order to mitigate those threats.

6 Was the output of the tool useful for you?

Yes, the output of the tool is useful for us. The output quickly provides us with all the potential threats that the design could generate. Although not all of them are accurate and easy to understand, most of them can give some insights on how vulnerable the design is.