RISK ASSESSMENT REPORT

Security Risk Assessment For

Smart(TB) portal

TABLE OF CONTENTS

LIST OF EXHIBITS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

Risk assessment participants:

Ahmed Yosry Akrab

Omar Ashraf Al-Ashmouny

Risk assessment techniques used:

checklist of known threats and hazards

Table A: Risk Classifications

Risk Level	Risk Description & Necessary Actions
High	**The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets or individuals.**
Moderate	**The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets or individuals.**
Low	**The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets or individuals.**

2 Identify and Prioritize Smart(TB) portal Assets

Table B: Smart(TB) portal assets

Priority	Asset	Asset information
2)	Website (Critical)	• Software • Technical security controls • Interfaces
1)	Servers (Critical)	• Information storage protection • IT Security architecture • Technical security controls
4)	Patient contact information (Low)	• Data • Users
5)	Doctors contact information (Medium)	• Data • Users
3)	Hospital lab sensitive X-ray dataset (Critical)	• Data

Figure 1 – Smart(TB) Portal System Boundary Diagram

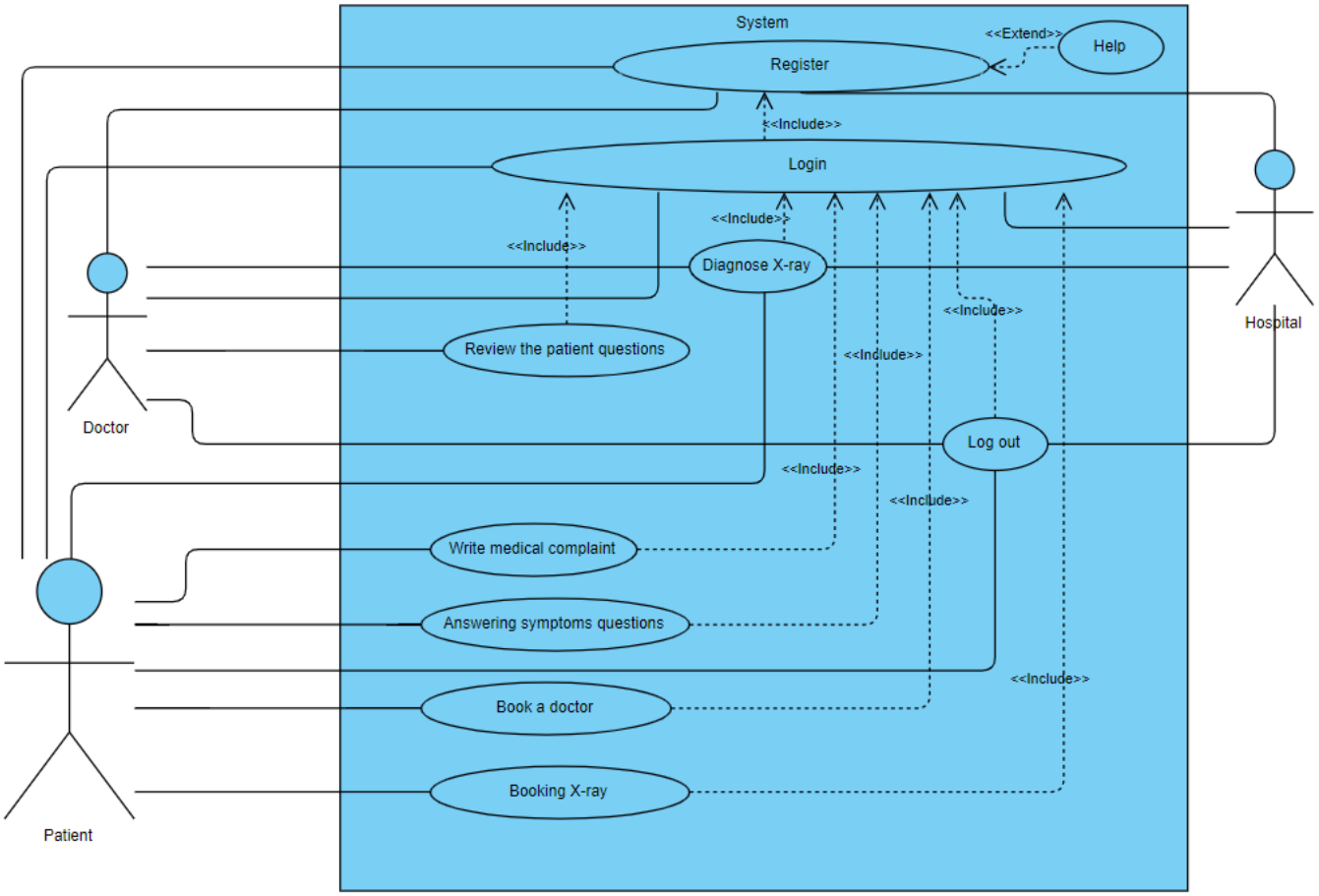
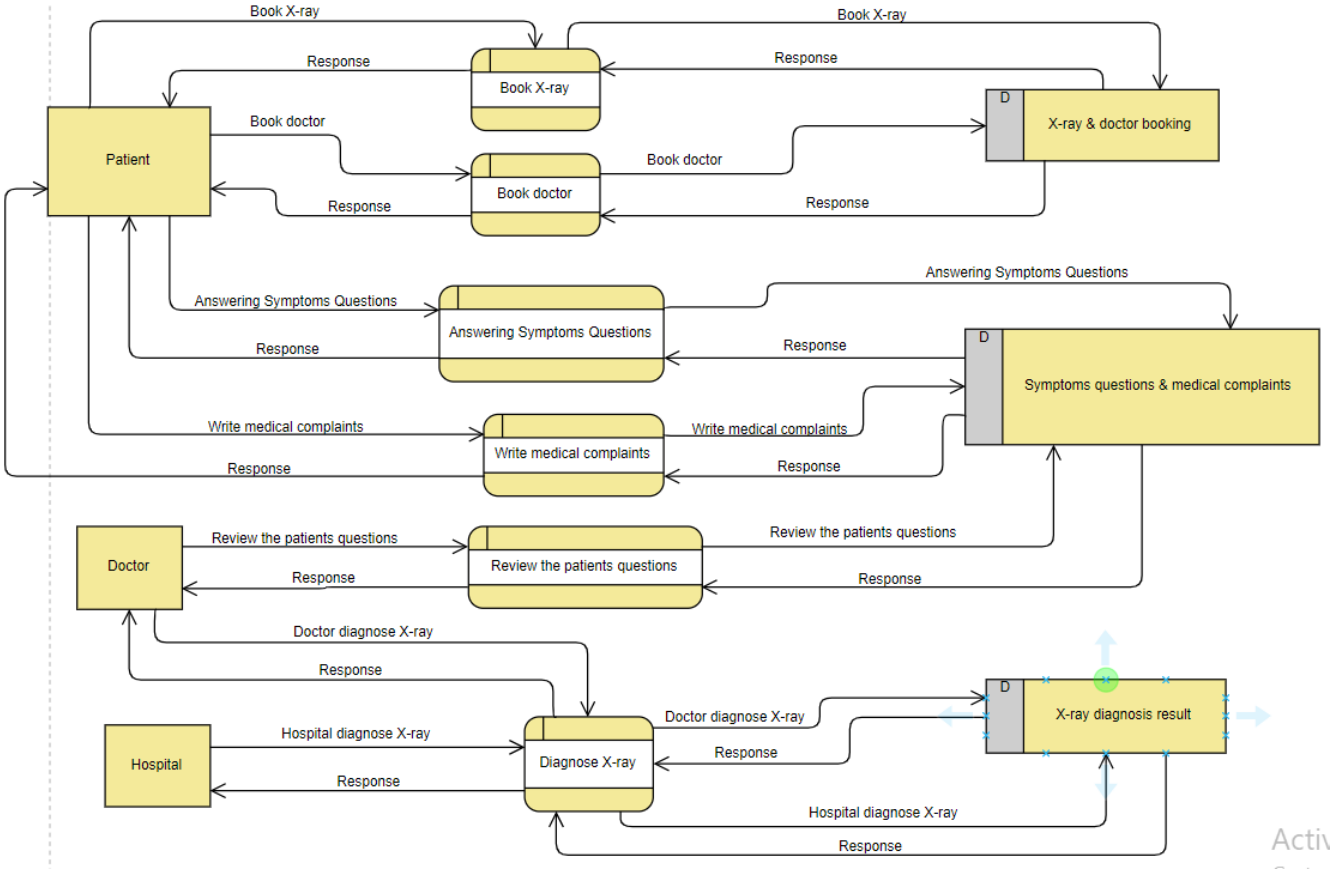


Figure 2 – Smart(TB) Portal Information Flow Diagram



3 Identify Threats

The threats identified are listed in Table C.

Table C: Threats Identified

Threat	Threat type(Category)	Threat identity
IP address spoofing to the servers	Malicious humans	Interception
Remote code execution to the website	Malicious humans	Interception
Data manipulation to the Hospital lab sensitive X-ray dataset	Accidental human interference	make mistakes e.g. (Accidentally deleting important files)
Sql Injection for Patient contact information	Malicious humans	Interception
Sql Injection for Doctors contact information	Malicious humans	Interception

4 Identify Vulnerabilities

The way vulnerabilities combine with credible threats to create risks is identified Table D.

Table D: Vulnerabilities, Threats, and Risks

Risk No.	Vulnerability	Threat	Risk of Compromise of	Risk Summary
1	***No Use of cryptographic network protocols***	*IP address spoofing to the servers*	***user data or spreading malware to harm users accounts***	*The attacker motivation is to launch attacks against network hosts, steal data, spread malware or bypass access controls*
2	***NO timely installation of software update***	Remote code execution *to the website*	***Website performance and confidentiality***	*When the attacker gain a user administrative access, the attacker can do any fraud or any other illegal actions.*
3	***NO regularly back up to our data***	*Data manipulation to the Hospital lab sensitive X-ray dataset*	***Hospital lab sensitive X-ray dataset***	*Attacker will fraud the datasets so may an X-ray test result be wrong because of the inaccurate prediction due to the false dataset.*
4	***NO Parameterized queries in the portal system***	Sql Injection *for Patient contact information*	***Patient account personal data***	*Attacker motivation is to know secret info. of Patient to override their valuable data, or even to execute dangerous system level commands on the database host.*
5	***NO Parameterized queries in the portal system***	Sql Injection *for Doctors contact information*	***Doctor account personal data***	*Attacker motivation is to know secret info. of Doctor to override their valuable data, or even to execute dangerous system level commands on the database host.*

5 Analyze Controls

Table E documents the IT security controls in place and planned for the IT system.

Table E: Security Controls

Control Area	In-Place/ Planned	Description of Controls
1 Risk Management		
1.1 IT Security Roles & Responsibilities	Planned	***Owning SSL certification for our web application & using cloud services afford it to us.***
1.2 Business Impact Analysis	Planned	***Our business core idea and goals was discussed before, but in case of the lack of availability backups and fail over strategies will help us mitigates our technical problems to continue our business.***
1.3 IT System & Data Sensitivity Classification	Planned	***Owning SSL certification for our web application & using cloud services afford it to us.***
1.4 IT System Inventory & Definition	Planned	***Owning SSL certification for our web application & using cloud services afford it to us.***
1.5 Risk Assessment	In-Place	***After identifying our vulnerabilities we are now planning to control our risk assessment.***
1.6 IT Security Audits	Planned	***Owning SSL certification for our web application & using cloud services afford it to us.***
2 IT Contingency Planning		
2.1 Continuity of Operations Planning	Planned	***Owning SSL certification for our web application & using cloud services afford it to us.***
2.2 IT Disaster Recovery Planning	Planned	***Owning SSL certification for our web application & using cloud services afford it to us.***
2.3 IT System & Data Backup & Restoration	Planned	***Owning SSL certification for our web application & using cloud services afford it to us.***
3 IT Systems Security		
3.1 IT System Hardening	Planned	***Smart(TB) portal doesn't contain hardware as a part of it as it is a medical diagnosis system depending on cloud services.***

Control Area	In-Place/ Planned	Description of Controls
3.2 IT Systems Interoperability Security	In-Place	***After identifying our vulnerabilities we are now planning to control our risk assessment to protect* Interoperability quality attribute.**
3.3 Malicious Code Protection	In-Place	***We are planning to timely install software update, this ranks as the top cybersecurity measure in preventing remote or malicious code execution attacks.***
3.4 IT Systems Development Life Cycle Security	***In-Place***	***We are planning to apply a suitable framework e.g. (ITIL framework).***
4 Logical Access Control		
4.1 Account Management	***Planned***	***It was planned in our prototype***
4.2 Password Management	***Planned***	***It was planned in our prototype***
4.3 Remote Access	***Planned***	***It was planned in our prototype***
5 Data Protection		
4.4 Data Storage Media Protection	***Planned***	***Owning SSL certification for our web application & using cloud services afford it to us.***
4.5 Encryption	***Planned***	***Owning SSL certification for our web application & using cloud services afford it to us.***
6 Facilities Security		
6.1 Facilities Security	***Planned***	***Owning SSL certification for our web application & using cloud services afford it to us.***
7 Personnel Security		
7.1 Access Determination & Control	***Planned***	***Owning SSL certification for our web application & using cloud services afford it to us.***
7.2 IT Security Awareness & Training	***In-Place***	***We are planning to design tutorials to all our portal users to know well how to use it and protect well their info. .***
7.3 Acceptable Use	***Planned***	***Owning SSL certification for our web application & using cloud services afford it to us.***
8 Threat Management		
8.1 Threat Detection	***Planned***	***Owning SSL certification for our web application & using cloud services afford it to us.***
8.2 Incident Handling	***In-Place***	***We are handling it in our security risk assessment.***
8.3 Security Monitoring & Logging	***Planned***	***Owning SSL certification for our web application & using cloud services afford it to us.***
9 IT Asset Management		
9.1 IT Asset Control	***In-Place***	***We are planning to many controls to handle our IT Asset***
9.2 Software License Management	***Planned***	**Software License for users is for free until now and for us we manage our services availability by renewing our ownership to the *SSL certification for our web application & our cloud services.***

Control Area	In-Place/ Planned	Description of Controls
9.3 Configuration Management & Change Control	***Planned***	***This configuration criteria changes according to the change of our business criteria.***

Table E correlates the risks identified in Table C with relevant IT security controls documented in Table D and with other mitigating or exacerbating factors.

Table F: Risks-Controls-Factors Correlation

Risk No.	Risk Summary	Correlation of Relevant Controls & Other Factors
1	*The attacker motivation is to launch attacks against network hosts, steal data, spread malware or bypass access controls*	Controls should be preventive
2	*When the attacker gain a user administrative access, the attacker can do any fraud or any other illegal actions.*	Controls should be preventive
3	*Attacker will fraud the datasets so may an X-ray test result be wrong because of the inaccurate prediction due to the false dataset.*	Controls should be preventive
4	*Attacker motivation is to know secret info. of Patient to override their valuable data, or even to execute dangerous system level commands on the database host.*	Controls should be detective
5	*Attacker motivation is to know secret info. of Doctor to override their valuable data, or even to execute dangerous system level commands on the database host.*	Controls should be detective

6 Determine the Likelihood of an Incident

Table G defines the risk likelihood ratings.

Table G: Risk Likelihood Definitions

Effectiveness of Controls	Probability of Threat Occurrence (Natural or Environmental Threats) or Threat Motivation and Capability (Human Threats)		
	Low	Moderate	High
Low	Medium	High	High
Moderate	Low	Medium	High
High	Low	Low	Medium

Table G, evaluates the effectiveness of controls and the probability or motivation and capability of each threat to BFS and assigns a likelihood, as defined in Table F, to each risk documented in Table C.

Table H: Risk Likelihood Ratings

Risk No.	Risk Summary	Risk Likelihood Evaluation	Risk Likelihood Rating
1	*The attacker motivation is to launch attacks against network hosts, steal data, spread malware or bypass access controls*	**High**	**High**
2	*When the attacker gain a user administrative access, the attacker can do any fraud or any other illegal actions.*	**High**	**High**
3	*Attacker will fraud the datasets so may an X-ray test result be wrong because of the inaccurate prediction due to the false dataset.*	**High**	**High**
4	*Attacker motivation is to know secret info. of Patient to override their valuable data, or even to execute dangerous system level commands on the database host.*	**Low**	**Low**
5	*Attacker motivation is to know secret info. of Doctor to override their valuable data, or even to execute dangerous system level commands on the database host.*	**Medium**	**Medium**

7 Assess the Impact a Threat Could Have

Table I documents the ratings used to evaluate the impact of risks.

Table I: Risk Impact Rating Definitions

Magnitude of Impact	Impact Definition
High	**Occurrence of the risk: (1) May result in human death or serious injury; (2) May result in the loss of major tangible assets, resources or sensitive data; or (3) May significantly harm, or impede the mission, reputation or interest.**
Medium	**Occurrence of the risk: (1) May result in human injury; (2) May result in the costly loss of tangible assets or resources; or (3) May violate, harm, or impede the mission, reputation or interest.**
Low	**Occurrence of the risk: (1) May result in the loss of some tangible assets or resources or (2) May noticeably affect the mission, reputation or interest.**

Table J documents the results of the impact analysis, including the estimated impact for each risk identified in Table D and the impact rating assigned to the risk.

Table J: Risk Impact Analysis

Risk No.	Risk Summary	Risk Impact	Risk Impact Rating
1	*The attacker motivation is to launch attacks against network hosts, steal data, spread malware or bypass access controls*	**High**	**High** ***(2)***
2	*When the attacker gain a user administrative access, the attacker can do any fraud or any other illegal actions.*	**High**	**High** ***(3)***
3	*Attacker will fraud the datasets so may an X-ray test result be wrong because of the inaccurate prediction due to the false dataset.*	**High**	**High** ***(1)***

Risk No.	Risk Summary	Risk Impact	Risk Impact Rating
4	*Attacker motivation is to know secret info. of Patient to override their valuable data, or even to execute dangerous system level commands on the database host.*	**Low**	**Low** ***(2)***
5	*Attacker motivation is to know secret info. of Doctor to override their valuable data, or even to execute dangerous system level commands on the database host.*	**Medium**	**Medium** ***(1)***

8 Prioritize the Information Security Risks

Table K documents the criteria used in determining overall risk ratings.

Table K: Overall Risk Rating Matrix

Risk Likelihood	Risk Impact		
	Low (10)	Moderate (50)	High (100)
High (1.0)	Low 10 x 1.0 = 10	Moderate 50 x 1.0 = 50	High 100 x 1.0 = 100
Moderate (0.5)	Low 10 x 0.5 = 5	Moderate 50 x 0.5 = 25	Moderate 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Low 100 x 0.1 = 10

Risk Scale: Low (1 to 10); Moderate (>10 to 50); High (>50 to 100)

Table L assigns an overall risk rating, as defined in Table K, to each of the risks documented in Table D.

Table L: Overall Risk Ratings Table

Risk No.	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating
1	*The attacker motivation is to launch attacks against network hosts, steal data, spread malware or bypass access controls*	High	High	100 x 1.0 = 100
2	*When the attacker gain a user administrative access, the attacker can do any fraud or any other illegal actions.*	High	High	100 x 1.0 = 100
3	*Attacker will fraud the datasets so may an X-ray test result be wrong because of the inaccurate prediction due to the false dataset.*	High	High	100 x 1.0 = 100
4	*Attacker motivation is to know secret info. of Patient to override their valuable data, or even to execute dangerous system level commands on the database host.*	Low	Low	10 x 0.1 = 1

Risk No.	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating
5	*Attacker motivation is to know secret info. of Doctor to override their valuable data, or even to execute dangerous system level commands on the database host.*	**Medium**	**Medium**	**50 x 0.5 = 25**

9 Recommend Controls

Table M documents recommendations for the risks identified in Table D.

Table M: Recommendations

Risk No.	Risk	Risk Rating	Recommendations
1	**May result in the loss of major assets, resources or sensitive data**	**100**	**A mitigation activity for this threat is Use cryptographic network protocols: Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols bolster spoofing attack prevention efforts by encrypting data before it is sent and authenticating data as it is received.**
2	**May significantly harm, or impede the Portal mission, reputation or interest.**	**100**	***Timely patching or timely installation of software update ranks as the top cybersecurity measure in preventing remote code execution attacks. This the best mitigation activity for that threat.***
3	**May result in human death or serious health problems**	**100**	***we will use Jupyter Notebooks, the popular environment among data scientists, to predict the salaried class using both raw data and privacy-protected data. We will be using CryptoNumerics' privacy libraries for the privacy algorithms and sklearn for the regression.***
4	**May noticeably affect the Portal mission, reputation or interest.**	**1**	***A mitigation activity for this threat are Parameterized queries which are simple to write and understand. They force you to define the SQL query and use placeholders for user-provided variables in the query. After the SQL statement is defined, you can pass each parameter to the query. This allows the database to distinguish between the SQL command and data supplied by a user. If you properly parametrize SQL queries, all user input that is passed to the database is treated as data and can never be confused as being part of a command.***

5	**May result in serious health problems**	**25**	***A mitigation activity for this threat are Parameterized queries which are simple to write and understand. They force you to define the SQL query and use placeholders for user-provided variables in the query. After the SQL statement is defined, you can pass each parameter to the query. This allows the database to distinguish between the SQL command and data supplied by a user. If an attacker inputs SQL commands, the parameterized query treats them as untrusted input and the database does not execute injected SQL commands.***

10 Document the Results

Exhibit 1: Risk Assessment Matrix

Risk No.	Vulnerability	Threat	Risk	Risk Summary	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating	Analysis of Relevant Controls and Other Factors	Recommendations
1	***No Use of cryptographic network protocols***	**IP address spoofing to the servers**	**May result in the loss of major assets, resources or sensitive data**	*The attacker motivation is to launch attacks against network hosts, steal data, spread malware or bypass access controls*	**High**	**High**	**100**	Controls should be preventive	**A mitigation activity for this threat is Use cryptographic network protocols: Transport Layer Security (TLS), Secure Shell (SSH), HTTP Secure (HTTPS) and other secure communications protocols bolster spoofing attack prevention efforts by encrypting data before it is sent and authenticating data as it is received.**
2	***NO timely installation of software update***	**Remote code execution to the website**	**May significantly harm, or impede the Portal mission, reputation or interest.**	*When the attacker gain a user administrative access, the attacker can do any fraud or any other illegal actions.*	**High**	**High**	**100**	Controls should be preventive	***Timely patching or timely installation of software update ranks as the top cybersecurity measure in preventing remote code execution attacks. This the best mitigation activity for that threat.***

3	***NO regularly back up to our data***	**Data manipulation to the Hospital lab sensitive X-ray dataset**	**May result in human death or serious health problems**	*Attacker will fraud the datasets so may an X-ray test result be wrong because of the inaccurate prediction due to the false dataset.*	**High**	**High**	**100**	Controls should be preventive	***we will use Jupyter Notebooks, the popular environment among data scientists, to predict the salaried class using both raw data and privacy-protected data. We will be using CryptoNumerics' privacy libraries for the privacy algorithms and sklearn for the regression.***

4	***NO Parameterized queries in the portal system***	**Sql Injection for Patient contact information**	**May noticeably affect the Portal mission, reputation or interest.**	*Attacker motivation is to know secret info. of Patient to override their valuable data, or even to execute dangerous system level commands on the database host.*	**Low**	**Low**	**1**	Controls should be detective	***A mitigation activity for this threat are Parameterized queries which are simple to write and understand. They force you to define the SQL query and use placeholders for user-provided variables in the query. After the SQL statement is defined, you can pass each parameter to the query. This allows the database to distinguish between the SQL command and data supplied by a user. If you properly parametrize SQL queries, all user input that is passed to the database is treated as data and can never be confused as being part of a command.***

5	***NO Parameterized queries in the portal system***	**Sql Injection for Doctors contact information**	**May result in serious health problems**	*Attacker motivation is to know secret info. of Doctor to override their valuable data, or even to execute dangerous system level commands on the database host.*	**Medium**	**Medium**	**25**	Controls should be detective	***A mitigation activity for this threat are Parameterized queries which are simple to write and understand. They force you to define the SQL query and use placeholders for user-provided variables in the query. After the SQL statement is defined, you can pass each parameter to the query. This allows the database to distinguish between the SQL command and data supplied by a user. If an attacker inputs SQL commands, the parameterized query treats them as untrusted input and the database does not execute injected SQL commands.***