iriusrisk

Technical Threat Report

User Accounts

Report generated by:	Administrator admin
Unique ID:	user-accounts
Workflow State:	

Index

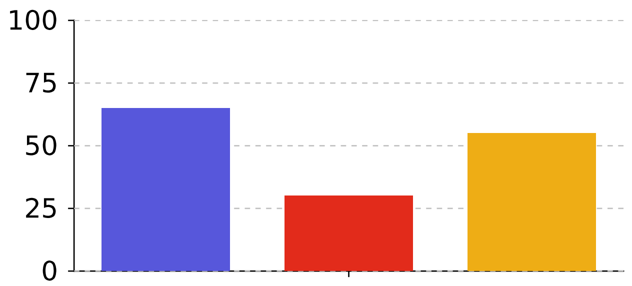
Summary

Shown below is a brief description of the product and summary analysis of the risks.

Product name:	User Accounts
Unique ID:	user-accounts
Product description:	
Business unit:	bu_user_admin
Owner:	Administrator admin

Risk Summary

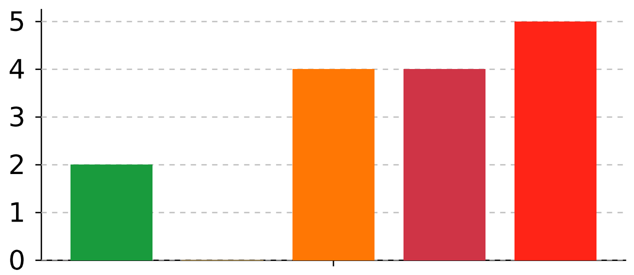
Current risk level compared with the inherent and projected risk levels.



🟦 Inherent Risk 🟥 Projected Risk
🟨 Current Risk

Risk Distribution

The number of threats in each risk rating level.



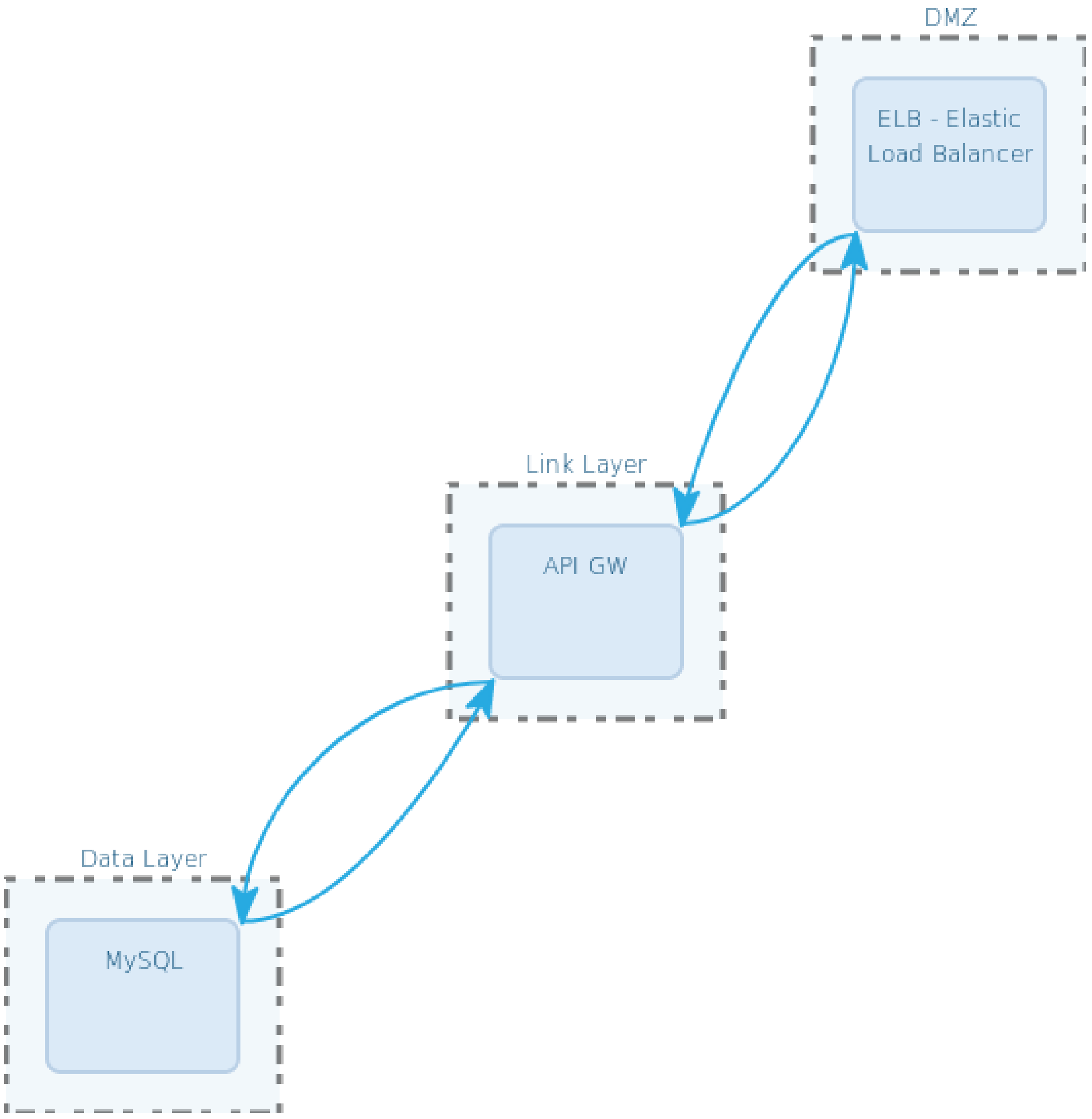
🟩 Very low 🟨 Low 🟧 Medium 🟥 High
🟥 Critical

Risk Mitigation Summary

The following table details the progress of threat mitigation per product.

Product name:	User Accounts
Inherent risk rating:	High (65)
Current risk rating:	High (55)
Projected risk rating:	Medium (29)
# Required countermeasures:	11
% Implemented countermeasures:	35 %
% Implemented countermeasures with failed tests:	0 %
# Vulnerabilities:	0

Architectural Diagrams



Filename: irius-risk-diagram-architecture-image.png
Username: admin **Date uploaded:** 09-May-2019 15:20:22

Unmitigated Threats:

Listed below are threats per component where all countermeasures are not implemented or the weaknesses test result failed.

Component: API GW

Threat name	Inherent Risk	Current Risk	Planned mitigation
Denial of service through resource exhaustion	Critical	Critical	0 %
Attackers gain control of the connection through a Man In The Middle attack	High	High	100 %
Attacks against the authentication system may go undetected	Medium	Medium	100 %
Attackers gain access to the system through Server Side Code Injection	Critical	Critical	100 %
Attackers gain control of the system through a source code leakage	High	High	0 %

Component: ELB - Elastic Load Balancer

Threat name	Inherent Risk	Current Risk	Planned mitigation
An attacker eavesdrops on the communication between the client and server and decrypts the data.	Critical	Critical	0 %
Attackers make undetected and unaudited changes in the resources	Critical	Critical	0 %
Attackers gain unauthorized connection to the resources	Critical	Critical	0 %

Component: MySQL

Threat name	Inherent Risk	Current Risk	Planned mitigation
Attackers obtain unauthorised access by connecting directly to the service	Medium	Medium	0 %
Attackers gain unauthorised access to data and/or systems through SQL Injection attacks	Medium	Medium	100 %
Attackers gain access to unauthorised data by exploiting vulnerabilities in the service	High	High	50 %

Partly-Mitigated Threats:

Listed below are threats per component where some countermeasures are not implemented or the weaknesses test result failed.

Component: API GW

Threat name	Inherent Risk	Current Risk	Planned mitigation	Current mitigation
Attackers subvert the intended workflow of the application in order to perform unauthorised operations	High	Medium	0 %	50 %
An attacker injects, manipulates or forges malicious log entries in the log file, allowing him to mislead a log audit, cover traces of attack, or perform other malicious actions	Critical	High	80 %	20 %

Mitigated Threats:

Below is the list of threats per component where all countermeasures are implemented and have passed their tests and there are no failed weakness tests.

Component: API GW

Threat name	Inherent Risk	Current Risk	Planned mitigation
Data leakage or disclosure to unauthorized parties	High	Very Low	0 %

Component: MySQL

Threat name	Inherent Risk	Current Risk	Planned mitigation
Attackers who compromise the application or application server could directly access and modify the data store	Medium	Very Low	0 %

Failed Countermeasure Tests:

Component: API GW

Limit the number of accounts with privileges allowing modification and/or deletion of audit logs files
Description: Limit the number of account with privileges to modify and/or delete audit logs files.
Test notes:
Related threats: CAPEC-93

Component: MySQL

Require authentication before presenting restricted data
Description: The application should ensure users have undergone an Identification and Verification (ID&V) process before allowing access to secret, sensitive or otherwise restricted data. For less sensitive but still restricted data, simple verification of the location of the user may suffice (e.g. IP restrictions). • For non-sensitive but non-public data, access could be restricted by IP address, for example limiting access to internal networks, workstations, or gateways • For more sensitive data, TLS client-side certificates may be appropriate • Where secret or other sensitive data is handled, a full authentication process to identify and validate users with single or multi-factor authentication may be required

Related threats: CAPEC-115

Appendix A: Threat Details

The number of threats in each risk rating level.

Component: API GW

Id	Name	Description	State
CWE-94	Attackers gain access to the system through Server Side Code Injection	Server Side Code Injection happens when an attacker is able to direct input under his control and mix it with executed code on server side by modifying the logic executed on it. Depending on the code isolation, this event could grant the user with access to system resources and data.	Exposed
CAPEC-130	Denial of service through resource exhaustion	An attacker causes the target to allocate excessive resources to servicing the attackers' request, thereby reducing the resources available for legitimate services and degrading or denying services. Usually, this attack focuses on memory allocation, but any finite resource on the target could be the attacked, including bandwidth, processing cycles, or other resources. This attack does not attempt to force this allocation through a large number of requests (that would be Resource Depletion through Flooding) but instead uses one or a small number of requests that are carefully formatted to force the target to allocate excessive resources to service this request(s). Often this attack takes advantage of a bug in the target to cause the target to allocate resources vastly beyond what would be needed for a normal request. For example, using an Integer Attack, the attacker could cause a variable that controls allocation for a request to hold an excessively large value. Excessive allocation of resources can render a service degraded or unavailable to legitimate users and can even lead to crashing of the target.	Exposed
SOURCE-LEAK	Attackers gain control of the system through a source code leakage	Attackers gain unauthorized access to a service by reading raw source code returned by the service, if this code contains confidential information such as authentication credentials or other secrets that can be used to access the service. Configuration files that can be downloaded from the service could also be used to gain access to sensitive information.	Exposed
CAPEC-300	Attackers gain control of the connection through a Man In The Middle attack	This type of attack targets the communication between two components (typically client and server). The attacker places himself in the communication channel between the two components. Whenever one component attempts to communicate with the other (data flow, authentication challenges, etc.), the data first goes to the attacker, who has the opportunity to observe or alter it, and it is then passed on to the other component as if it was never intercepted. This interposition is transparent leaving the two compromised components unaware of the potential corruption or leakage of their communications. The potential for Man-in-the-Middle attacks yields an implicit lack of trust in communication or identify between two components.	Exposed
CWE-778-AUTH	Attacks against the authentication system may go undetected	Automated attacks against many user accounts, or successful attacks against an account require a response. If audit logs are not kept of both successful and unsuccessful authentication operations, then post attack forensics will be hampered. Without a dynamic response to mass automated attacks against the authentication system, attackers stand a greater chance of success.	Exposed

EU-GDPR-DATA_LEAKAGE-UNAUTHZ-PARTIES	Data leakage or disclosure to unauthorized parties	Unauthorized party might access/breach the personal data of the data subject.	Mitigated
CAPEC-172	Attackers subvert the intended workflow of the application in order to perform unauthorised operations	If an application enforces an order in workflows, then attackers could attempt to bypass this order so that they can perform operations for which they are not authorized. The technique can also be used to gain access to unauthorized data.	Partly Mitigated
CAPEC-93	An attacker injects, manipulates or forges malicious log entries in the log file, allowing him to mislead a log audit, cover traces of attack, or perform other malicious actions	This attack targets the log files of the target host. The attacker injects, manipulates or forges malicious log entries in the log file, allowing him to mislead a log audit, cover traces of attack, or perform other malicious actions. The target host is not properly controlling log access. As a result tainted data is resulting in the log files leading to a failure in accountability, non-repudiation and incident forensics capability.	Partly Mitigated

Component: ELB - Elastic Load Balancer

Id	Name	Description	State
UNAUDITABLE-CHANGES-RESOURCES-AWS	Attackers make undetected and unaudited changes in the resources	If audit trails in the resources are not enabled or not protected, attackers could gain access to the system and modify or delete data from the resources and the changes are not detected.	Exposed
EAVESDROPPING-COMMUNICATIONS	An attacker eavesdrops on the communication between the client and server and decrypts the data.	Eavesdropping on communication is a network attack that captures small packets transmitted by other computers and reads the data content. This type of network attack is most effective when weak encryption services are used. An attacker could eavesdrop on the communication between the client and server and decrypt the encrypted data.	Exposed
UNAUTHORIZED-CONECTIONS-AWS	Attackers gain unauthorized connection to the resources	Attackers could gain an unauthorized connection to the resources through misconfigured ports or security network configurations.	Exposed

Component: MySQL

Id	Name	Description	State
CAPEC-66	Attackers gain unauthorised access to data and/or systems through SQL Injection attacks	Successful SQL Injection attacks could lead to full compromise of the database or to a partial compromise of only the data visible to the application. Typically, these types of attacks result in unauthorized disclosure of sensitive data, but can also be used to inject spurious data into the database or to drop tables and deny service to legitimate users.	Exposed
VULN-SERVICE	Attackers gain access to unauthorised data by exploiting vulnerabilities in the service	Attackers exploit vulnerabilities in the service and gain access to data, or to services for which they are not authorized.	Exposed
CAPEC-115	Attackers obtain unauthorised access by connecting directly to the service	If the component does not require authentication then an attacker can simply connect directly to the service to obtain the data. This risk may also apply to data that is not necessarily sensitive, but is non-public. For example, obtaining timely market information which is not freely available through any other service.	Exposed
AUTH-DATASTORE-LEAST-PRIV	Attackers who compromise the application or application server could directly access and modify the data store	If attackers gain access to the application or the application server, then they could directly access the data store using the privilege assigned to the application. If the data store user account used by the application has elevated privileges then this could allow attackers to perform unauthorized operations such as dropping tables, modifying the database schema or modifying data.	Mitigated