Incident Response Playbook

SQL INJECTION VULNERABILITY

(Section 4)

Viva la Vita Online

Contents

Introduction

Scope

This Incident Response Playbook navigates various stages of handling SQL Injection Vulnerability. This vulnerability can lead to a compromise of database applications containing records of customers, employees and company’s infrastructure. This Incident Response Handling Playbook will help to prepare, detect, evaluate and mitigate, recover, and post-incident response for SQL Injection vulnerability.

Audience

For the SQL injection, the following would be stakeholders:

- Chief Information Officer
- Chief Information Security Officer
- Incident Response Manager
- IT Security Analyst
- Network and Systems Engineer
- Application and E-commerce Specialist
- Legal and Compliance Advisor
- Communications and Public Relations Coordinator
- Human Resources Representative

Incident Response Team

This section will state the roles and responsibilities of the Computer Security Incident Response Team (CSIRT):

Incident Response Manager

- Spearhead and oversee the complete process of the incident response.
- Take critical decisions with respect to the SQL Injection incident and lead the CSIRT accordingly.
- Work with HR and PR Coordinator to ensure smooth and proper communication between CSIRT and affected stakeholders.

- Ensure that timely reporting is made between CSIRT members and CISO.

IT Security Analyst

- Identify and analyze SQL injection attack.
- Collaborate with Network and Systems Engineer and Application and E-commerce Specialist and gather information on the details of the attack.
- Work on the eradication and recovery process. Use range of methods and tools to analyze and perform threat intelligence and mitigation.
- Implement short term containment strategy to cut-off the attack effect.

Network and Systems Engineer

- Gather detailed information to find the attack details and provide it to the IT Security Analyst. Also, support in mitigating the attack.
- Limit the resources that are affected in the attack from the company's infrastructure, employee, and customers to maintain integrity.

Application and E-commerce Specialist

- Provide in-depth knowledge and technical specifications of the database application that is affected by SQL injection.
- Support in containment and eradication phases.

Legal and Compliance Advisor

- Work with the team to ensure legal and compliance regulations are being implemented.

Communications and Public Relations Coordinator

- Understand the nature of attack and analyze the affected entities and stakeholders.
- Communicate with IR manager and address the relevant updates to the internal and external entities regarding the incident.

Human Resources Representative

- Work with IR manager to address concerns regarding employees and their data.
- Ensure that company's rules and regulations are in compliance with the incident response and it's processes.
- Communicate with employees and provide the relevant updates and support regarding the situation.

Note : Team members should be prepared to adapt their roles based on dynamic situation and circumstances.

Preparation

Tools

1. **Security Information and Event Management (SIEM)** - IBM QRadar 7.5
2. **Perimeter Firewall on the network egress points** - Fortinet FortiGate 7.4
3. **Intrusion Prevention Sensors on the internal network** - Suricata 6.0.15
4. **Vulnerability Patching Management** - Tenable Nessus 10.6

Resources and Strategies

- Database Backup at specific time intervals. At the times of SQL Injection, revert to the latest database copy.
- Risk assessment to be performed at regular periods.
- Secure Coding practices should be implemented. Awareness and training sessions should be conducted.
- Input validation of users to ensure unexpected characters and statements.
- Database Server exposed to the public should not have root level access.
- SQL queries should be parameterized in order to avoid malicious inputs and escalation of access to the resources of the database.
- Monitor the queries from the web server and flag the suspicious activities and inputs.
- Keep updated version of the tools used for the incident response.
- Take the web snapshots. At the time of the SQL injection, shift the affected web application to the unaffected snapshot.
- Perform Dynamic Application Security Testing (DAST) to determine any SQL vulnerability in the web application prior to hosting it.

Communication Channels

- Ticketing ecosystem to report an incident and track it.
- Encrypted mail system to communicate between the team.

Note : Team members should be prepared to adapt their roles based on dynamic situation and circumstances.

Identification

Detection

SIEM	Alerts for potential SQL injection queries. Perform regular log analysis. Turn on intrusion prevention sensors.
IDS/IPS	Similar to SIEM, it triggers notification and alerts. False positives are possible. Check the triggered event manually and escalate the incident accordingly.
WAF	Unusual and suspicious web traffic should be blocked having SQL injection patterns.
Web Vulnerability Management	In-depth scanning of website of SQL injection vulnerabilities.

Reporting

Through Network Control tools, incident should be notified and reported to the team members of the potential SQL injection. Prioritized alert regarding the injection should be sent containing details of the incident.

The details should at least have:

- Packet dump
- Source and Destination IP
- Geotags of the IP
- Resources accessed and affected
- SQL query parameters

Initial Assessment Procedure

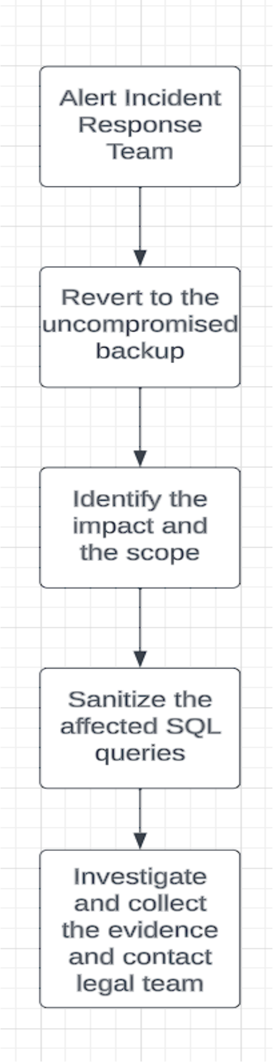
Steps for Initial Assessment are:

1. Receive Incident Alert and start triage procedures
2. Analyze SIEM Logs
3. Assess SQL Injection queries (Lexical Analyzer etc.)
4. Determine Impact and Scope
5. Report to Incident Response Manager

Priority (Low to High)	Description
P1	Non-essential resources are affected that does not affect business continuity for short period of time.
P2	Exploitation of website elements like product price, description etc.
P3	Effecting clients and retailers account and profile.
P4	Effecting administrator accounts and databases.

Containment

Short-term Containment Strategies


Alert Incident Response Team
Revert to the uncompromised backup
Identify the impact and the scope
Sanitize the affected SQL queries
Investigate and collect the evidence and contact legal team

Long-term Containment Measures

- Regular system patching should be carried out.
- Continuous monitoring of all the logs and web application traffic.
- Secure coding practices should be implemented.
- Perform Interactive Application Security Testing.
- Use manual testing of SQL queries.

Eradication

Root Cause Analysis

- Perform Vulnerability Analysis and Assessment to determine which vulnerabilities have been exploited by the threat agent.
- Check what resources have been exploited by an attacker.

Eradication Procedures

Steps to eradicate the SQL injection attack:

1. Sanitize the SQL query that was exploited.
2. Add validation and input sanitization methods.
3. Update Security controls from the findings of investigation to mitigate such threats in the future.

Recovery

System Restoration Process

- Restore the web application to the latest snapshot prior to the attack with the SQL sanitization methods implemented.

- Check the lost data like orders, account creation and modifications and apply those changes.
- If some changes made are private to the user, notify them about the incident and guide them for further process.

Validation Checks

- Using Interactive Application Security Testing (IAST) verify that sanitized SQL changes are working.
- Use similar SQL injection queries and analyze the traffic with the resulting modifications.
- Refer security modules and standards to implement rigorous SQL parameterized queries.
- Validate the restored data and check for any incomplete or corrupt data.

Ongoing Monitoring:

- Enable STEALTH modes on the IBM QRadar 7.5 .
- At specific intervals verify all the network and host controls.
- From P4-P1 priority check each resources and validate their actual state with required state.

Post-Incident Activity

Lessons Learned Session

- Hold secure coding training sessions.
- Send regular security updates on web vulnerabilities.
- Make awareness of various web vulnerabilities that can be found in Viva La Vita Online.
- Check on regular updates of tools and resources used for defensive measures.

Incident Report Writing

- Include SQL Injection parameters that were used to exploit.
- Mention what resources were compromised.
- Provide a theoretical and practical walkthrough of the attack for better understanding.
- Write the SQL sanitized query.
- Details of the packet dump, Ips and their geolocations, and HTTPS headers.
- Include each and every action with timestamps from identification to recovery.

Appendices

Legal and Compliance Guidelines:

- Contact federal authorities as soon as the incident is identified and detected. Notify them regarding the incident and cooperate with whatever required.
- Follow NIST 800-171 for evidence preservation and retention for reporting unauthorized to the authorities.
- In compliance with Data Protection Laws, follow the standards and requirements.

Contact Information:

Internal Contact:

Incident Response Manager
+1 (395)-154-3245

IT Security Analyst
+1 (395)-035-9845

Network and Systems Engineer
+1 (395)-984-6516

Application and E-commerce Specialist
+1 (395)-466-6025

External Contact / Law Enforcement :

FBI - +1 (395)-566-9985

IC3 - +1 (988)-754-4682

CISA - +1 (741)-485-1200

BLACKLISTED IP SEEN IN VPN CONNECTIONS

(Section 7)

Viva la Vita Online

Contents

Introduction

Scope

This Incident Response Playbook navigates various stages of handling Blacklisted IP seen in VPN connections. This scenario can lead to a compromise of database applications containing records of customers, employees and company's infrastructure by escalating privileges or getting unauthorized access. This Incident Response Handling Playbook will help to prepare, detect, evaluate and mitigate, recover, and post-incident response for Blacklisted IP seen in VPN connections.

Assumption

This playbook is for j.saw and any accounts that has same privileges.

Audience

The following would be team and stakeholders:

- Incident Response Manager
- IT Security Analyst
- Network and Systems Engineer
- Application and E-commerce Specialist
- Legal and Compliance Advisor
- Communications and Public Relations Coordinator
- Human Resources Representative

Incident Response Team

This section will state the roles and responsibilities of the Computer Security Incident Response Team (CSIRT):

Incident Response Manager

- Spearhead and oversee the complete process of the incident response.

- Take critical decisions with respect to the Blacklisted IP seen in VPN connections incident and lead the CSIRT accordingly.
- Work with HR and PR Coordinator to ensure smooth and proper communication between CSIRT and affected stakeholders.
- Ensure that timely reporting is made between CSIRT members and CISO.

IT Security Analyst

- Identify and analyze the incident.
- Collaborate with Network and Systems Engineer and Application and E-commerce Specialist and gather information on the details of the attack.
- Work on the eradication and recovery process. Use range of methods and tools to analyze and perform threat intelligence and mitigation.
- Implement short term containment strategy to cut-off the attack effect.

Network and Systems Engineer

- Gather detailed information to find the attack details and provide it to the IT Security Analyst. Also, support in mitigating the attack.
- Limit the resources that are affected in the attack from the company's infrastructure, employee, and customers to maintain integrity.

Application and E-commerce Specialist

- Provide in-depth knowledge and technical specifications of the web application.
- Support in containment and eradication phases.

Legal and Compliance Advisor

- Work with the team to ensure legal and compliance regulations are being implemented.

Communications and Public Relations Coordinator

- Understand the nature of attack and analyze the affected entities and stakeholders.
- Communicate with IR manager and address the relevant updates to the internal and external entities regarding the incident.

Human Resources Representative

- Work with IR manager to address concerns regarding employees and their data.
- Ensure that company's rules and regulations are in compliance with the incident response and it's processes.
- Communicate with employees and provide the relevant updates and support regarding the situation.

Note : Team members should be prepared to adapt their roles based on dynamic situation and circumstances.

Preparation

Tools and Resources

Security Information and Event Management (SIEM) - IBM QRadar 7.5

- Monitor SIEM logs merged with VPN connections. Update rules and configuratiions accordingly to prevent emerging threats.

Perimeter Firewall on the network egress points - Fortinet FortiGate 7.4

- Monitor the network traffic. Keep updating the blacklisted IP list. Update rules and configuratiions accordingly to prevent emerging threats.

Intrusion Prevention Sensors on the internal network - Suricata 6.0.15

- Deploy configurations that flags the unusual activities. Check

Anti-malware Endpoint Protection on all devices - Symantec Endpoint Protection Client for Windows 14.3

- Detecting malware elements in any communication channels or network traffic.
- Symantec Endpoint Protection Client for Windows 14.3

Symantec Endpoint Protection Client for Windows 14.3 - Bitlocker for Windows 10 and 11 versions devices

- Post attack, protects the data of employees and company's infrastructure.

Communication Channels

- Ticketing ecosystem to report an incident and track it.
- Encrypted mail system to communicate between the team.

Note : Team members should be prepared to adapt their communication channels based on dynamic situation and circumstances.

Identification

Detection

SIEM	Alerts for blacklisted IP connecting to the server. Perform regular log analysis. Turn on intrusion prevention sensors.
IDS/IPS	Similar to SIEM, it triggers notification and alerts. False positives are possible. Check the triggered event manually and escalate the incident accordingly.
WAF	Unusual and suspicious web traffic should be blocked and reviewed.

Reporting

Through Network Control tools incidents should be notified and reported to the team members of the potential unauthorized access. Prioritized alert regarding the access should be sent containing details of the incident.

The details should at least have:

- Logs while attack was attempted
- Packet dump
- Source and Destination IP
- Geotags of the IP
- Resources accessed and affected

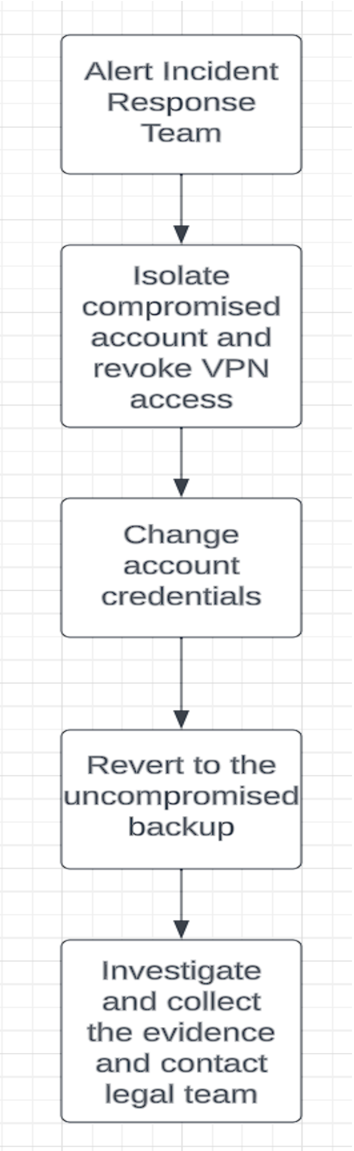
Initial Assessment Procedure

Steps for Initial Assessment are:

1. Receive Incident Alert and start triage procedures
2. Analyze SIEM and VPN logs
3. Determine Impact and Scope
4. Report to Incident Response Manager

Containment

Short-term Containment Strategies


Alert Incident Response Team
Isolate compromised account and revoke VPN access
Change account credentials
Revert to the uncompromised backup
Investigate and collect the evidence and contact legal team

Long-term Containment Measures

- Disable the escalated account j.saw.
- Disable BitLocker to see the source of the unauthorized access.
- Identify the resources and elements accessed in the attack.

- Shift the internal communications to another mode and channels.
- Delete the malicious actions taken by the compromised account.

Eradication

Root Cause Analysis

- Monitor VPN and SIEM logs, and network traffic for unusual activities.
- Geographical irregularities found.
- Any unintended modifications in the web application and it's infrastructure.
- Check the user's account activity to identify the source of unauthorized access.

Eradication Procedures

Steps to eradicate the incident:

1. Change the affected account's credentials.
2. Regular system patching should be carried out.
3. Implement MFA at each user login interface.

Recovery

System Restoration Process

- Revert to the latest uncompromised backup of the system.
- Enable BitLocker to encrypt the data. Internal communication channels should be encrypted too.

Validation Checks:

- Assess the VPN connection along with security controls and configuration.
- Verify new password hashes with the leaked hashes.
- Refer security modules and standards.
- Check all the configuration and controls of the web application and infrastructure.

Ongoing Monitoring

- Enable STEALTH modes on the IBM QRadar 7.5 .
- At specific intervals verify all the network and host controls.
- Monitor network traffic for malicious and suspicious activity.

Post-Incident Activity

Lessons Learned Session

- Implement the principle of least privilege.
- Hold awareness sessions guiding appropriate password standards.
- Send regular notifications to update the password.
- Compare the password hashes with the leaked hashes and send the alerts accordingly.
- Check on regular updates of tools and resources used for defensive measures.
-

Incident Report Writing

- Mention what resources were compromised.
- Provide a theoretical and practical walkthrough of the attack for better understanding.
- Details of the packet dump, IPs and their geolocations, and HTTPS headers.

Appendices

Legal and Compliance Guidelines:

- Contact federal authorities as soon as the incident is identified and detected. Notify them regarding the incident and cooperate with whatever required.
- Follow NIST 800-171 for evidence preservation and retention for reporting unauthorized to the authorities.
- In compliance with Data Protection Laws, follow the standards and requirements.

Contact Information:

Internal Contact:

Incident Response Manager
+1 (395)-154-3245

IT Security Analyst
+1 (395)-035-9845

Network and Systems Engineer
+1 (395)-984-6516

Application and E-commerce Specialist
+1 (395)-466-6025

External Contact / Law Enforcement:

FBI - +1 (395)-566-9985

IC3 - +1 (988)-754-4682

CISA - +1 (741)-485-1200