Relatório Geral de Incidente de Segurança - Sistema SEMED

1. Introdução

No dia 21 de Abril de 2025, foi detectado um incidente de segurança no sistema SEMED, envolvendo tentativas de ataque por meio de SQL Injection, onde comandos maliciosos foram inseridos em campos de entrada.

2. Descrição dos Ataques

Foram identificadas cargas maliciosas como 'PG_SLEEP(15)', 'waitfor delay', e 'OR 1=1'. Essas cargas tinham como objetivo travar o banco de dados, explorar falhas e comprometer a disponibilidade do sistema. Foram encontrados 244 registros contaminados.

3. Análise Técnica

O ataque foi realizado explorando a falta de sanitização adequada nos campos de formulários. Apesar disso, o uso correto do ORM Django evitou a execução direta dos comandos maliciosos no banco. Sessões de usuários foram auditadas e não indicaram envolvimento interno no ataque.

4. Ações Corretivas Imediatas

- Backup completo do banco de dados e logs.
- Implementação de script de scanner de IPs suspeitos.
- Auditoria de sessões em django_session.
- Isolamento do sistema e restrição de cadastros temporariamente.

5. Medidas de Fortalecimento

- Criação de Middleware global para sanitização e proteção contra SQL Injection.
- Reforço de segurança no settings.py com HTTPS, cookies seguros e CSRF.
- Aplicação de blacklist de comandos maliciosos em campos de entrada.
- Bloqueio de IPs suspeitos detectados nos logs.

6. Resultados Obtidos

O incidente foi contido, nenhuma evidência de acesso indevido ao banco foi identificada além dos registros

contaminados. O sistema foi endurecido contra novas tentativas de SQL Injection e mecanismos de monitoramento foram ativados.

7. Conclusão

O ataque foi mitigado com sucesso e diversas melhorias de segurança foram implementadas. O sistema encontra-se protegido com camadas adicionais de segurança, e políticas de auditoria e resposta a incidentes foram iniciadas.