Missão Prática | Nível 5 | Mundo 5

Italo Augusto Juliano Barbosa - 202303617674

Campus Aparecida de Goiânia
Nível 3: Software Sem Segurança Não Serve – 9001 – 5º Semestre
Link do repositório no GitHub: https://github.com/Anarquia122/trabalho-facul-SoftwareSeguro

Objetivo da Prática

1. Descrever o controle básico de acesso a uma API Rest;
2. Descrever o tratamento de dados sensíveis e log de erros com foco em segurança;
3. Descrever a prevenção de ataques de acesso não autorizado com base em tokens desprotegidos/desatualizados;
4. Descrever o tratamento de SQL Injection em códigos-fonte;
5. Descrevero tratamento de CRLF Injection em códigos-fonte;
6. Descrever a prevenção a ataques do tipo CSRF em sistemas web;

Contextualização:

O time de segurança da Software House, onde você atua como Especialista em Desenvolvimento de Software, identificou uma falha de segurança, explorada por ataques que geraram o vazamento de dados, além de outros problemas, em uma das aplicações legadas, desenvolvida há alguns anos atrás. Tal falha consiste na concessão de acesso não autorizado de recursos a usuários. O cenário completo é descrito a seguir:

A aplicação web possui um frontend e um backend, sendo esse último

uma API Rest. O padrão geral da estrutura de URLs (e URI) da aplicação é:

- http://dominio.com/nome-do-recurso/{session-id}
- http://dominio.com/nome-do-recurso/{id}/{session-id}

O padrão acima é usado tanto no frontend, no navegador, como no backend, nos endpoints.

Após uma simples análise, foi identificado que o valor do parâmetro "session-id" é obtido com a encriptação do id do usuário logado no sistema, usando um processo suscetível a falhas, uma vez que um dos principais dados necessários no processo de criptografia é o próprio nome da empresa detentora do software.

Logo, tal falha é passível de ser explorada via ataques de força bruta para descoberta do padrão usado na geração da "session-id" e consequente geração de valores aleatórios que serão usados para a realização de requisições – como solicitações de dados e também criação e atualização – na aplicação, até a obtenção do acesso indevido.

Além do problema já relatado, o time de segurança descobriu que, atualmente, não é realizado nenhum tratamento no processamento dos parâmetros trafegados na aplicação. Logo, também é possível explorar outras falhas, como as de "Injection" de códigos maliciosos.