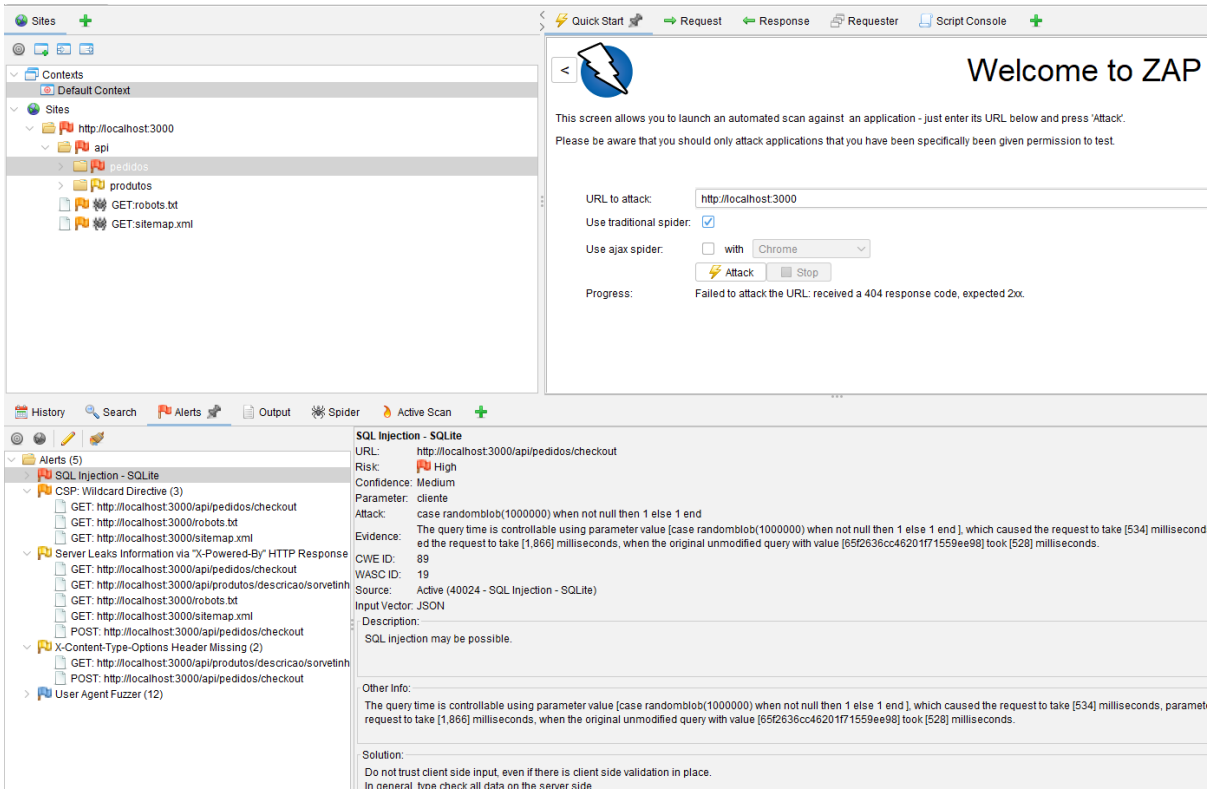
Análise OWASP ZAP

Como solicitado, foi feito a análise pela ferramenta ZAP dos end-points indicados.

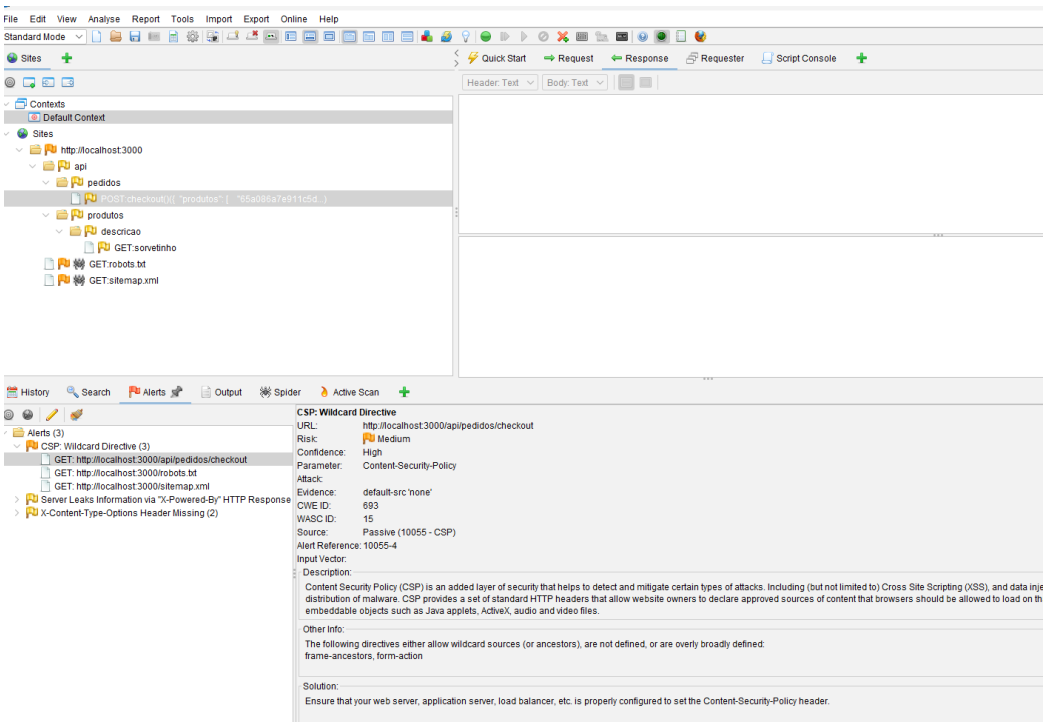
End-Points:

- **Solicitação de Pedido:** a análise indicou um alert de alta criticidade, onde foi identificado uma falha de segurança para SQL Injection, por conta de tempo de execução que era diferente dependendo do tipo de ataque e isso gera uma brecha

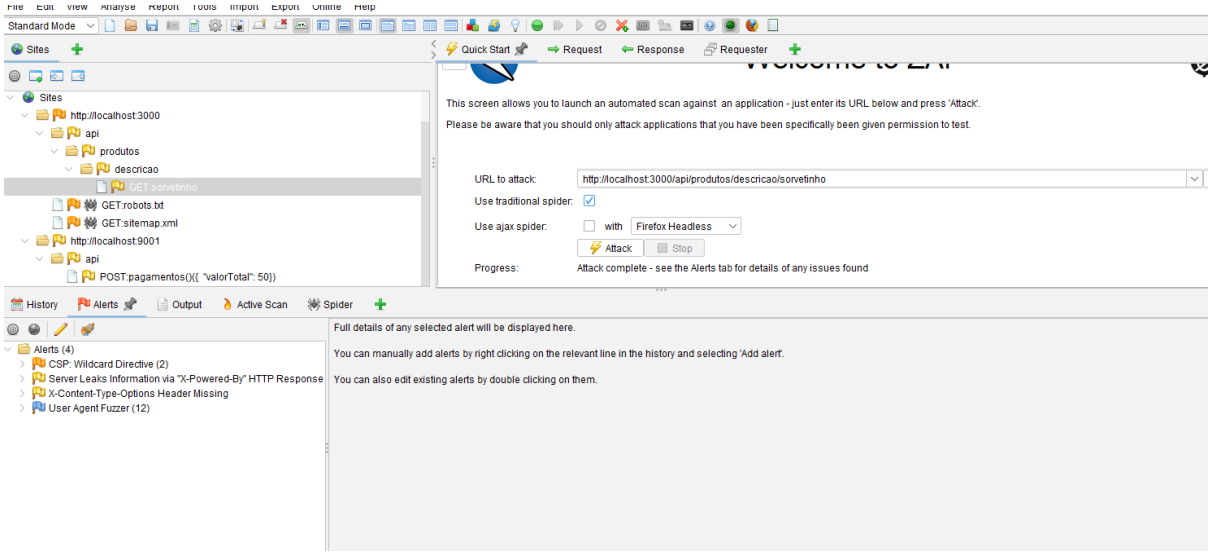


Como correção foi aplicado um time limite para controlar essa requisição. Após a correção, foi executado o scan novamente e já não consta com a falha.

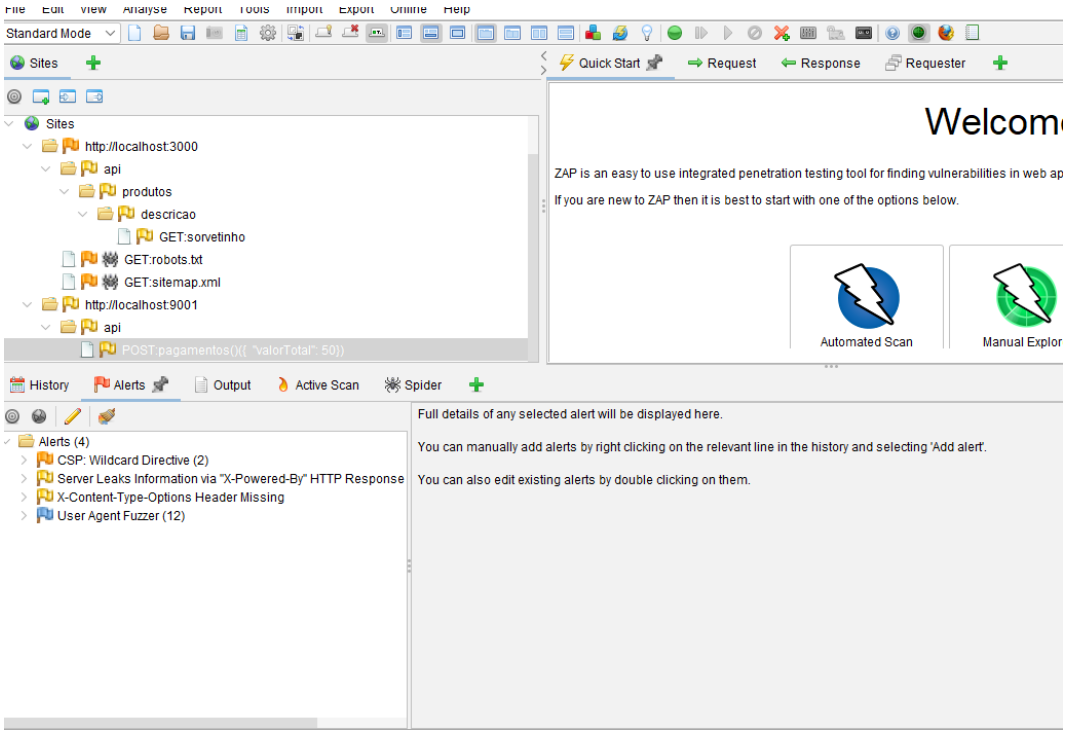
```
const TIMEOUT_LIMIT = 900; // Limite de tempo em milissegundos (5 segundos)

const timeoutMiddleware = (req: Request, res: Response, next: Function) => {
    // Define um temporizador para o limite de tempo
    const timeout = setTimeout(() => {
        // Se o tempo limite for atingido, retorna uma resposta de erro 500
        res.status(500).send({ message: 'Tempo limite excedido ao processar a requisição.' });
    }, TIMEOUT_LIMIT);

    // Função para limpar o temporizador
    const clearTimer = () => clearTimeout(timeout);

    // Adiciona a função clearTimer ao objeto de resposta para garantir que o temporizador seja limpo
    res.on('finish', clearTimer);
    res.on('close', clearTimer);

    // Passa a execução para o próximo middleware ou rota
    next();
};
```



- **Listar Cardápio:** Foi executado a análise scan para a requisição, entretanto não foi encontrado nenhum tipo de vulnerabilidade alta. Portanto não foi necessário ajustes a serem feitos.



- **Geração pagamento:** Foi executado a análise scan para a requisição, entretanto não foi encontrado nenhum tipo de vulnerabilidade alta. Portanto não foi necessário ajustes a serem feitos.



- **Confirmação de pagamento:** Foi executado a análise scan para a requisição, entretanto não foi encontrado nenhum tipo de vulnerabilidade alta. Portanto não foi necessário ajustes a serem feitos.