

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

The screenshot displays the OWASP ZAP (Zed Attack Proxy) interface. The top section shows the 'Welcome to ZAP' screen with a 'Quick Start' button and instructions for launching an automated scan. The 'URL to attack' is set to 'http://localhost:3000'. The 'Use traditional spider' checkbox is checked, and the 'Use ajax spider' checkbox is unchecked. The 'Attack' button is highlighted.

The bottom section shows the 'Alerts' pane, which lists several alerts. The first alert is 'SQL Injection - SQLite', which is highlighted. The details for this alert are as follows:

- URL:** http://localhost:3000/api/pedidos/checkout
- Risk:** High
- Confidence:** Medium
- Parameter:** cliente
- Attack:** case randomblob(1000000) when not null then 1 else 1 end
- Evidence:** The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [534] milliseconds, when the original unmodified query with value [65f2636cc46201f71559ee98] took [528] milliseconds.
- CWE ID:** 89
- WASC ID:** 19
- Source:** Active (40024 - SQL Injection - SQLite)
- Input Vector:** JSON
- Description:** SQL injection may be possible.
- Other Info:** The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [534] milliseconds, parameter request to take [1,866] milliseconds, when the original unmodified query with value [65f2636cc46201f71559ee98] took [528] milliseconds.
- Solution:** Do not trust client side input, even if there is client side validation in place. In general, *never* check all data on the server side.

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);

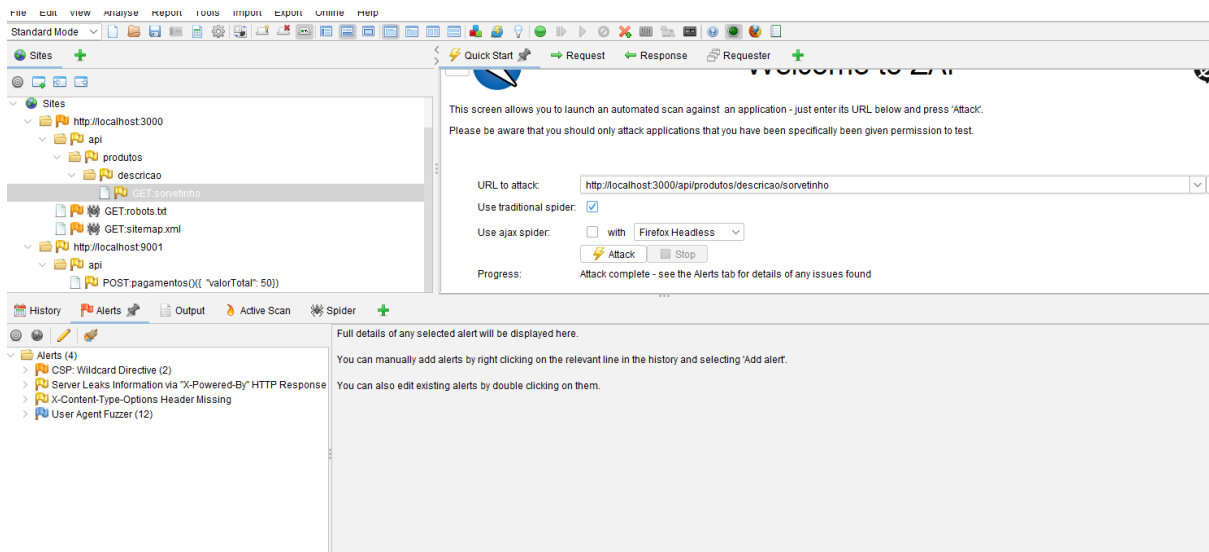
  // Adiciona a função clearTimer ao objeto de resposta para garantir que o temporizador seja limpo
  res.on('finish', clearTimer);
  res.on('close', clearTimer);

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

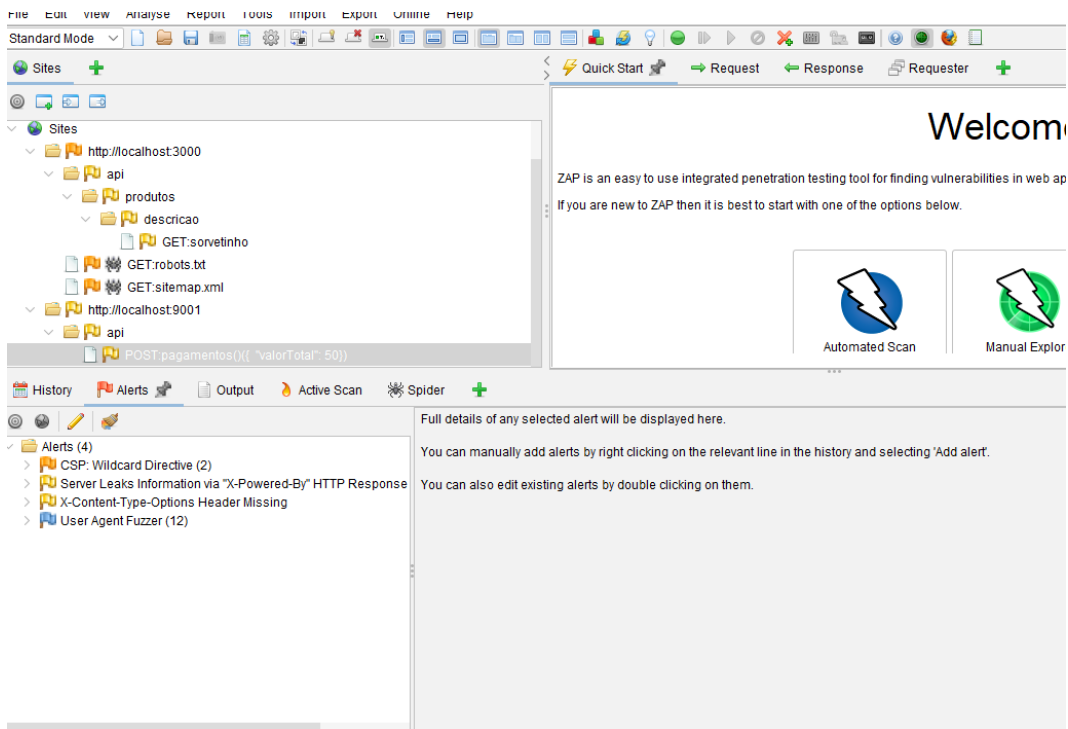
The screenshot displays the Burp Suite application interface. The top menu bar includes File, Edit, View, Analyse, Report, Tools, Import, Export, Online, and Help. The main workspace is divided into several panes. On the left, the 'Sites' pane shows a tree structure of the scanned site, including 'http://localhost:3000' with sub-paths like 'api', 'pedidos', 'produtos', and 'descricao'. The 'Alerts' pane at the bottom left lists three alerts, with the first one, 'CSP: Wildcard Directive (3)', selected. The right pane provides detailed information about the selected alert, including its URL, risk level, confidence, and a description of the Content Security Policy (CSP) issue.

CSP: Wildcard Directive	
URL:	http://localhost:3000/api/pedidos/checkout
Risk:	Medium
Confidence:	High
Parameter:	Content-Security-Policy
Attack:	
Evidence:	default-src 'none'
CWE ID:	693
WASC ID:	15
Source:	Passive (10055 - CSP)
Alert Reference:	10055-4
Input Vector:	
Description:	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on the web page. This prevents the execution of malicious scripts, even if included on the page by a third party. Other content types (such as images, stylesheets, etc.) are also protected against cross-domain attacks.
Other Info:	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action
Solution:	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

- **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.

