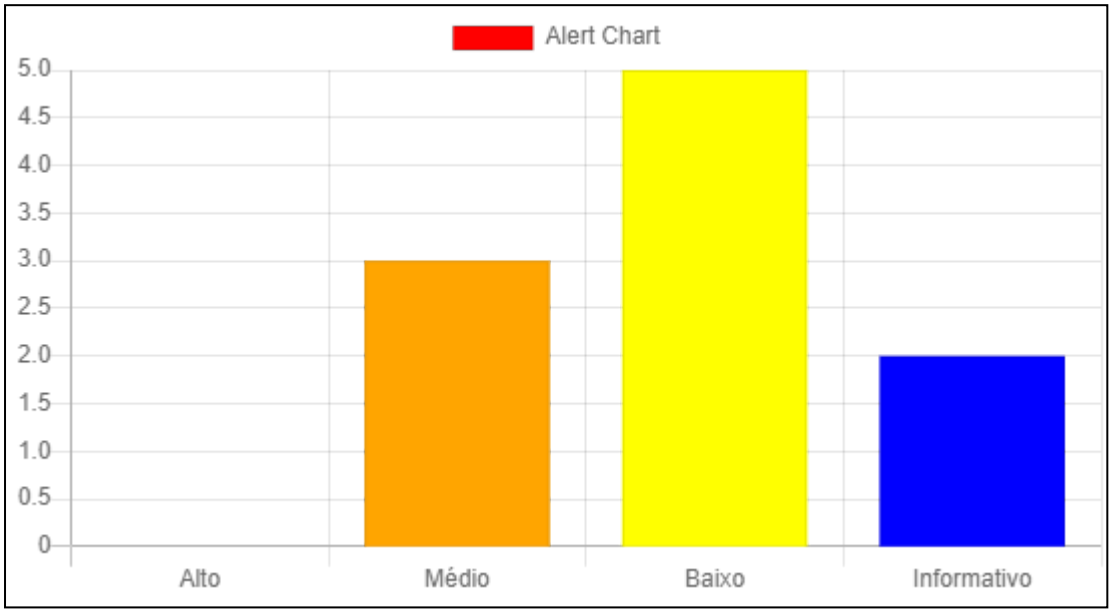
# ZAP Scanning Report

### Generated on qui., 8 ago. 2024 10:48:21

### ZAP Version: 2.15.0

**ZAP is supported by the Crash Override Open Source Fellowship**




## Summary of Alerts

| Nível de Risco | Number of Alerts |
|---|---|
| Alto | 0 |
| Médio | 3 |
| Baixo | 5 |
| Informativo | 2 |

## Alertas

| Nome | Nível de Risco | Number of Instances |
|---|---|---|
| Content Security Policy (CSP) Header Not Set | Médio | 1 |
| Erro de Formato de String | Médio | 1 |
| Missing Anti-clickjacking Header | Médio | 1 |
| Fraqueza de script entre sites (persistente na resposta JSON) | Baixo | 1 |
| O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By" | Baixo | 9 |
| Server Leaks Version Information via "Server" HTTP Response Header Field | Baixo | 1 |
| Strict-Transport-Security Header Not Set | Baixo | 12 |
| X-Content-Type-Options Header Missing | Baixo | 6 |
| Re-examine Cache-control Directives | Informativo | 6 |

| | | |
|---|---|---|
| User Agent Fuzzer | Informativo | 42 |

## Passing Rules

| Nome | Rule Type | Threshold | Strength |
|---|---|---|---|
| Navegação no Diretório | Active | MEDIUM | MEDIUM |
| Injeção CRLF | Active | MEDIUM | MEDIUM |
| Travessia/Passagem de Caminho | Active | MEDIUM | MEDIUM |
| Inclusão de Arquivo Remoto | Active | MEDIUM | MEDIUM |
| Adulteração de parâmetros | Active | MEDIUM | MEDIUM |
| Incluir Lado do Servidor | Active | MEDIUM | MEDIUM |
| GET for POST | Active | MEDIUM | MEDIUM |
| Cross Site Scripting (Refletido) | Active | MEDIUM | MEDIUM |
| Regras de Varredura Ativa | Active | MEDIUM | MEDIUM |
| Cross Site Scripting (Persistente) - Primário | Active | MEDIUM | MEDIUM |
| Cross Site Scripting (Persistente) - Spider | Active | MEDIUM | MEDIUM |
| Injeção SQL | Active | MEDIUM | MEDIUM |
| Injeção SQL - MySQL | Active | MEDIUM | MEDIUM |
| Injeção SQL - Hypersonic SQL | Active | MEDIUM | MEDIUM |
| Injeção SQL - Oracle | Active | MEDIUM | MEDIUM |
| Injeção SQL - PostgreSQL | Active | MEDIUM | MEDIUM |
| Injeção SQL - SQLite | Active | MEDIUM | MEDIUM |
| Cross Site Scripting (baseado em DOM) | Active | MEDIUM | MEDIUM |
| Injeção SQL - MsSQL | Active | MEDIUM | MEDIUM |
| Vazamento de Informação ELMAH | Active | MEDIUM | MEDIUM |
| Trace.axd Vazamento de Informação | Active | MEDIUM | MEDIUM |
| Injeção XSLT | Active | MEDIUM | MEDIUM |
| Vazamento de informações .htaccess | Active | MEDIUM | MEDIUM |
| .env Information Leak | Active | MEDIUM | MEDIUM |
| Injeção de Código no Lado do Servidor | Active | MEDIUM | MEDIUM |
| Hidden File Finder | Active | MEDIUM | MEDIUM |
| Injeção XPath | Active | MEDIUM | MEDIUM |
| Injeção Remota de Comandos de SO | Active | MEDIUM | MEDIUM |
| XML External Entity Attack | Active | MEDIUM | MEDIUM |
| Oracle Padding Genérico | Active | MEDIUM | MEDIUM |
| Spring Actuator Information Leak | Active | MEDIUM | MEDIUM |
| Spoofing de Ação SOAP | Active | MEDIUM | MEDIUM |
| Log4Shell | Active | MEDIUM | MEDIUM |
| Injeção de SOAP XML | Active | MEDIUM | MEDIUM |
| Spring4Shell | Active | MEDIUM | MEDIUM |
| Vulnerabilidade OpenSSL Heartbleed | Active | MEDIUM | MEDIUM |
| Estouro de Buffer | Active | MEDIUM | MEDIUM |
| Divulgação de Código-Fonte - CVE-2012-1823 | Active | MEDIUM | MEDIUM |
| Server Side Template Injection | Active | MEDIUM | MEDIUM |

| | | | |
|---|---|---|---|
| Execução Remota de Código - CVE-2012-1823 | Active | MEDIUM | MEDIUM |
| Metadados de nuvem potencialmente expostos | Active | MEDIUM | MEDIUM |
| Redirecionamento Externo | Active | MEDIUM | MEDIUM |
| Server Side Template Injection (Blind) | Active | MEDIUM | MEDIUM |
| Source Code Disclosure - /WEB-INF Folder | Active | MEDIUM | MEDIUM |
| Session Management Response Identified | Passive | MEDIUM | - |
| Verification Request Identified | Passive | MEDIUM | - |
| Private IP Disclosure | Passive | MEDIUM | - |
| Session ID in URL Rewrite | Passive | MEDIUM | - |
| Script Served From Malicious Domain (polyfill) | Passive | MEDIUM | - |
| Viewstate JSF Inseguro | Passive | MEDIUM | - |
| Vulnerable JS Library (Powered by Retire.js) | Passive | MEDIUM | - |
| Má Combinação de Charset | Passive | MEDIUM | - |
| Cookie No HttpOnly Flag | Passive | MEDIUM | - |
| Cookie Without Secure Flag | Passive | MEDIUM | - |
| Cross-Domain JavaScript Source File Inclusion | Passive | MEDIUM | - |
| Content-Type Header Missing | Passive | MEDIUM | - |
| Application Error Disclosure | Passive | MEDIUM | - |
| Divulgação de informações - Mensagens de Erro de Depuração | Passive | MEDIUM | - |
| Information Disclosure - Sensitive Information in URL | Passive | MEDIUM | - |
| Divulgação de Informações - Informações Confidenciais no Cabeçalho de Referência HTTP | Passive | MEDIUM | - |
| Divulgação de Informações - Comentários Suspeitos | Passive | MEDIUM | - |
| Open Redirect | Passive | MEDIUM | - |
| Cookie Poisoning | Passive | MEDIUM | - |
| User Controllable Charset | Passive | MEDIUM | - |
| Detecção de arquivo WSDL | Passive | MEDIUM | - |
| User Controllable HTML Element Attribute (Potential XSS) | Passive | MEDIUM | - |
| Cookie com Escopo Fraco | Passive | MEDIUM | - |
| Viewstate | Passive | MEDIUM | - |
| Navegação no Diretório | Passive | MEDIUM | - |
| Heartbleed OpenSSL Vulnerability (Indicative) | Passive | MEDIUM | - |
| X-Backend-Server Header Information Leak | Passive | MEDIUM | - |
| Secure Pages Include Mixed Content | Passive | MEDIUM | - |
| HTTP to HTTPS Insecure Transition in Form Post | Passive | MEDIUM | - |
| HTTPS to HTTP Insecure Transition in Form Post | Passive | MEDIUM | - |
| User Controllable JavaScript Event (XSS) | Passive | MEDIUM | - |
| Big Redirect Detected (Potential Sensitive Information Leak) | Passive | MEDIUM | - |
| Retrieved from Cache | Passive | MEDIUM | - |
| X-ChromeLogger-Data (XCOLD) Header Information Leak | Passive | MEDIUM | - |

| | | | |
|---|---|---|---|
| Cookie without SameSite Attribute | Passive | MEDIUM | - |
| CSP | Passive | MEDIUM | - |
| Vazamento de Informações do X-Debug-Token | Passive | MEDIUM | - |
| Hash de Nome de Usuário Encontrado | Passive | MEDIUM | - |
| X-AspNet-Version Response Header | Passive | MEDIUM | - |
| PII Disclosure | Passive | MEDIUM | - |
| Regras de Script de Varredura Passiva | Passive | MEDIUM | - |
| Estatísticas de Regra de Varredura Passiva | Passive | MEDIUM | - |
| Ausência de tokens Anti-CSRF | Passive | MEDIUM | - |
| Divulgação de Data e Hora | Passive | MEDIUM | - |
| Hash Disclosure | Passive | MEDIUM | - |
| Configuração Incorreta Entre Domínios | Passive | MEDIUM | - |
| Método Fraco de Autenticação | Passive | MEDIUM | - |
| Reverse Tabnabbing | Passive | MEDIUM | - |
| Modern Web Application | Passive | MEDIUM | - |
| Authentication Request Identified | Passive | MEDIUM | - |

# Sites

**Number of Sites tree nodes actively scanned:** 17

## https://i8z10k6wma.execute-api.us-east-1.amazonaws.com

| HTTP Response Code | Number of Responses |
|---|---|
| 403 Forbidden | 4 |
| 404 Not Found | 887 |
| 200 OK | 86 |
| 201 Created | 182 |
| 400 Bad Request | 1536 |
| 401 Unauthorized | 467 |
| 500 Internal Server Error | 28 |

**No Authentication Statistics Found**

| Parameter Name | Type | Flags | Times Used | # Values |
|---|---|---|---|---|

## Alert Detail

| Médio | Content Security Policy (CSP) Header Not Set |
|---|---|
| Descrição | Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution 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 that page — covered types are |

| | |
|---|---|
| | JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files. |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/payment/toggle |
| Método | PUT |
| Parameter | |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 288 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 214 bytes. | |
| Corpo de Resposta - size: 33 bytes. | |
| Instances | 1 |
| Solution | Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header. |
| Reference | https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy<br>https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html<br>https://www.w3.org/TR/CSP/<br>https://w3c.github.io/webappsec-csp/<br>https://web.dev/articles/csp<br>https://caniuse.com/#feat=contentsecuritypolicy<br>https://content-security-policy.com/ |
| Marcadores (Tags) | CWE-693<br>OWASP_2021_A05<br>OWASP_2017_A06 |
| CWE Id | 693 |
| WASC Id | 15 |
| Plugin Id | 10038 |

| **Médio** | **Erro de Formato de String** |
|---|---|
| Descrição | Um erro de Formato de String ocorre quando o dado enviado de uma string de entrada é avaliado como um comando pelo aplicativo. |

| | |
|---|---|
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | POST |
| Parameter | slug |
| Ataque | ZAP %1!s%2!s%3!s%4!s%5!s%6!s%7!s%8!s%9!s%10!s%11!s%12!s%13!s%14!s%15!s%16!s%17!s%18!s%19!s%20!s%21!n%22!n%23!n%24!n%25!n%26!n%27!n%28!n%29!n%30!n%31!n%32!n%33!n%34!n%35!n%36!n%37!n%38!n%39!n%40!n |
| Evidence | |
| Other Info | Possível Erro de Formato de String. O script fechou a conexão devido a um erro de formato de string da Microsoft |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 338 bytes. | |
| Corpo da Solicitação - size: 283 bytes. | |
| Cabeçalho de Resposta - size: 266 bytes. | |
| Corpo de Resposta - size: 52 bytes. | |
| Instances | 1 |
| Solution | Reescreva o programa de plano de fundo utilizando o apagamento apropriado das bad character strings. Isso irá requerer uma recompilação do executável do plano de fundo. |
| Reference | https://owasp.org/www-community/attacks/Format_string_attack |
| Marcadores (Tags) | OWASP_2017_A01<br>CWE-134<br>OWASP_2021_A03 |
| CWE Id | 134 |
| WASC Id | 6 |
| Plugin Id | 30002 |

| **Médio** | **Missing Anti-clickjacking Header** |
|---|---|
| Descrição | The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks. |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/payment/toggle |
| Método | PUT |
| Parameter | x-frame-options |

| | |
|---|---|
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 288 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 214 bytes. | |
| Corpo de Resposta - size: 33 bytes. | |
| Instances | 1 |
| Solution | Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.<br><br>If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive. |
| Reference | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options |
| Marcadores (Tags) | WSTG-v42-CLNT-09<br>OWASP_2021_A05<br>OWASP_2017_A06<br>CWE-1021 |
| CWE Id | 1021 |
| WASC Id | 15 |
| Plugin Id | 10020 |

| **Baixo** | **Fraqueza de script entre sites (persistente na resposta JSON)** |
|---|---|
| Descrição | Um ataque XSS foi encontrado em uma resposta JSON, isso pode deixar os consumidores de conteúdo vulneráveis a ataques se eles não manipularem os dados (resposta) de forma adequada. |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | slug |
| Ataque | <script>alert(1);</script> |
| Evidence | |

| | |
|---|---|
| Other Info | Gerado com BAIXA confiança, pois o Tipo de conteúdo não é HTML |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 284 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 252 bytes. | |
| Corpo de Resposta - size: 10.894 bytes. | |
| Instances | 1 |
| Solution | Fase: Arquitetura e Design.<br><br>Use uma biblioteca verificada ou framework que não permita que essa vulnerabilidade ocorra, ou forneça construções/implementações que tornem essa vulnerabilidade mais fácil de evitar.<br><br>Exemplos de bibliotecas e frameworks que facilitam a geração de saída codificada adequadamente incluem a biblioteca Anti-XSS da Microsoft, o módulo de codificação OWASP ESAPI e o Apache Wicket.<br><br>Fases: Implementação \| Arquitetura e Design.<br><br>Compreenda o contexto no qual seus dados serão usados e a codificação que será esperada. Isso é especialmente importante ao transmitir dados entre componentes diferentes ou ao gerar saídas que podem conter várias codificações ao mesmo tempo, como páginas da web ou mensagens de e-mail com várias partes. Estude todos os protocolos de comunicação e representações de dados esperados para determinar as estratégias de codificação necessárias.<br><br>Para quaisquer dados que serão enviados para outra página da web, especialmente quaisquer dados recebidos de entradas externas, use a codificação apropriada em todos os caracteres não alfanuméricos.<br><br>Consulte a Página de Dicas de Prevenção de XSS para obter mais detalhes sobre os tipos de codificação e escape que são necessários.<br><br>Fase: Arquitetura e Design.<br><br>Para todas as verificações de segurança realizadas no lado do cliente, certifique-se de que essas verificações sejam duplicadas no lado do servidor, a fim de evitar a CWE-602. Invasores podem ignorar as verificações do lado do cliente, modificando os valores após a realização das verificações ou alterando o cliente para remover as verificações do lado do cliente completamente. Em seguida, esses valores modificados poderiam ser enviados ao servidor.<br><br>Se disponível, use mecanismos estruturados que impõem automaticamente a separação entre dados e código. Esses mecanismos podem ser capazes de fornecer citação, codificação e validação relevantes automaticamente, em vez de depender do desenvolvedor para fornecer esse recurso em cada ponto onde a saída é gerada. |

| | |
|---|---|
| | Fase: Implementação.<br><br>Para cada página web gerada, use e especifique uma codificação de caracteres, como ISO-8859-1 ou UTF-8. Quando uma codificação não é especificada, o navegador pode escolher uma codificação diferente, tentando adivinhar por eliminação qual codificação está realmente sendo usada pela página da web. Isso pode fazer com que o navegador da web trate certas sequências como especiais, abrindo o cliente para ataques XSS sutis. Consulte a CWE-116 para obter mais informações sobre mitigações relacionadas à codificação/escape.<br><br>Para ajudar a mitigar os ataques XSS contra cookie de sessão do usuário, defina o cookie de sessão como HttpOnly. Em navegadores que suportam o recurso HttpOnly (como versões mais recentes do Internet Explorer e Firefox), esse atributo pode impedir que o cookie de sessão do usuário seja acessível a scripts mal-intencionados do lado do cliente que usam document.cookie. Esta não é uma solução completa, já que HttpOnly não é compatível com todos os navegadores. Mais importante ainda, XMLHTTPRequest e outras poderosas tecnologias de navegadores fornecem acesso de leitura a cabeçalhos HTTP, incluindo o cabeçalho Set-Cookie no qual o sinalizador HttpOnly é definido.<br><br>Presuma que toda a entrada de dados é maliciosa. Use uma estratégia de validação de entrada "aceita como boa", ou seja, use uma lista de permissões de entradas aceitáveis que estejam estritamente em conformidade com as especificações. Rejeite quaisquer entradas que não estejam estritamente de acordo com as especificações ou transforme-as em algo que esteja. Não confie exclusivamente na procura de entradas maliciosas ou malformadas (ou seja, não confie em uma lista de negação). No entanto, as listas de negação podem ser úteis para detectar ataques em potencial ou determinar quais entradas estão tão malformadas que devem ser rejeitadas imediatamente.<br><br>Ao executar a validação de entradas de dados, considere todas as propriedades potencialmente relevantes, incluindo comprimento, tipo de entrada, a gama completa de valores aceitáveis, entradas ausentes ou extras, sintaxe, consistência entre campos relacionados e conformidade com as regras de negócios. Como um exemplo de lógica de regra de negócios, "barco" pode ser sintaticamente válido porque contém apenas caracteres alfanuméricos, mas não é válido se você estiver esperando cores como "vermelho" ou "azul".<br><br>Certifique-se de realizar a validação de entrada em interfaces bem definidas dentro do aplicativo. Isso ajudará a proteger o aplicativo, mesmo se um componente for reutilizado ou movido para outro lugar. |
| Reference | https://owasp.org/www-community/attacks/xss/<br>https://cwe.mitre.org/data/definitions/79.html |
| Marcadores (Tags) | CWE-79<br>WSTG-v42-INPV-02<br>OWASP_2021_A03<br>OWASP_2017_A07 |
| CWE Id | 79 |
| WASC Id | 8 |
| Plugin Id | 40014 |

| **Baixo** | **O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By"** |
|---|---|
| Descrição | O servidor da web/aplicativo está vazando informações por meio de um ou mais cabeçalhos de resposta HTTP "X-Powered-By". O acesso a essas informações pode facilitar que os invasores identifiquem outras estruturas/componentes dos quais seu aplicativo da web depende e as vulnerabilidades às quais esses componentes podem estar sujeitos. |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | |
| Ataque | |
| Evidence | X-Powered-By: Express |

| | |
|---|---|
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 284 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 249 bytes. | |
| Corpo de Resposta - size: 499 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers |
| Método | GET |
| Parameter | |
| Ataque | |
| Evidence | X-Powered-By: Express |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 283 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 245 bytes. | |
| Corpo de Resposta | |

| | |
|---|---|
| - size: 2 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/GET/orders/:id |
| Método | GET |
| Parameter | |
| Ataque | |
| Evidence | X-Powered-By: Express |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 288 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 254 bytes. | |
| Corpo de Resposta - size: 40 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/orders |
| Método | GET |
| Parameter | |
| Ataque | |
| Evidence | X-Powered-By: Express |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 280 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |

| | |
|---|---|
| Cabeçalho de Resposta - size: 257 bytes. | |
| Corpo de Resposta - size: 43 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/products |
| Método | GET |
| Parameter | |
| Ataque | |
| Evidence | X-Powered-By: Express |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 282 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 249 bytes. | |
| Corpo de Resposta - size: 494 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | POST |
| Parameter | |
| Ataque | |
| Evidence | X-Powered-By: Express |
| Other Info | |
| Show / hide Request and Response | |

| | |
|---|---|
| Cabeçalho de Solicitação - size: 337 bytes. | |
| Corpo da Solicitação - size: 91 bytes. | |
| Cabeçalho de Resposta - size: 256 bytes. | |
| Corpo de Resposta - size: 63 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers |
| Método | POST |
| Parameter | |
| Ataque | |
| Evidence | X-Powered-By: Express |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 337 bytes. | |
| Corpo da Solicitação - size: 178 bytes. | |
| Cabeçalho de Resposta - size: 256 bytes. | |
| Corpo de Resposta - size: 77 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/orders |
| Método | POST |
| Parameter | |

| | |
|---|---|
| Ataque | |
| Evidence | X-Powered-By: Express |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 334 bytes. | |
| Corpo da Solicitação - size: 105 bytes. | |
| Cabeçalho de Resposta - size: 257 bytes. | |
| Corpo de Resposta - size: 43 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/products |
| Método | POST |
| Parameter | |
| Ataque | |
| Evidence | X-Powered-By: Express |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 336 bytes. | |
| Corpo da Solicitação - size: 206 bytes. | |
| Cabeçalho de Resposta - size: 256 bytes. | |

| | |
|---|---|
| Corpo de Resposta - size: 95 bytes. | |
| Instances | 9 |
| Solution | Certifique-se de que seu servidor web, servidor de aplicativos, balanceador de carga, etc. esteja configurado para suprimir cabeçalhos "X-Powered-By". |
| Reference | https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework<br>https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html |
| Marcadores (Tags) | OWASP_2021_A01<br>OWASP_2017_A03<br>WSTG-v42-INFO-08<br>CWE-200 |
| CWE Id | 200 |
| WASC Id | 13 |
| Plugin Id | 10037 |

| **Baixo** | **Server Leaks Version Information via "Server" HTTP Response Header Field** |
|---|---|
| Descrição | The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to. |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/payment/toggle |
| Método | PUT |
| Parameter | |
| Ataque | |
| Evidence | Werkzeug/2.2.2 Python/3.10.14 |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 288 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 214 bytes. | |
| Corpo de Resposta - size: 33 bytes. | |
| Instances | 1 |

| | |
|---|---|
| Solution | Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details. |
| Reference | https://httpd.apache.org/docs/current/mod/core.html#servertokens<br>https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)<br>https://www.troyhunt.com/shhh-dont-let-your-response-headers/ |
| Marcadores (Tags) | OWASP_2021_A05<br>OWASP_2017_A06<br>WSTG-v42-INFO-02<br>CWE-200 |
| CWE Id | 200 |
| WASC Id | 13 |
| Plugin Id | 10036 |

| **Baixo** | **Strict-Transport-Security Header Not Set** |
|---|---|
| Descrição | HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797. |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 284 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 249 bytes. | |
| Corpo de Resposta - size: 499 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers |
| Método | GET |
| Parameter | |

| | |
|---|---|
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 283 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 245 bytes. | |
| Corpo de Resposta - size: 2 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/GET/orders/:id |
| Método | GET |
| Parameter | |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 288 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 254 bytes. | |

| | |
|---|---|
| Corpo de Resposta - size: 40 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/orders |
| Método | GET |
| Parameter | |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 280 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 257 bytes. | |
| Corpo de Resposta - size: 43 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/products |
| Método | GET |
| Parameter | |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 282 bytes. | |
| Corpo da Solicitaçã | |

| | |
|---|---|
| o - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 249 bytes. | |
| Corpo de Resposta - size: 494 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |
| Parameter | |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 331 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 177 bytes. | |
| Corpo de Resposta - size: 485 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | POST |
| Parameter | |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request | |

| | |
|---|---|
| and Response | |
| Cabeçalho de Solicitação - size: 337 bytes. | |
| Corpo da Solicitação - size: 91 bytes. | |
| Cabeçalho de Resposta - size: 256 bytes. | |
| Corpo de Resposta - size: 63 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers |
| Método | POST |
| Parameter | |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 337 bytes. | |
| Corpo da Solicitação - size: 178 bytes. | |
| Cabeçalho de Resposta - size: 256 bytes. | |
| Corpo de Resposta - size: 77 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |

| | |
|---|---|
| Parameter | |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 343 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 177 bytes. | |
| Corpo de Resposta - size: 289 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/orders |
| Método | POST |
| Parameter | |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 334 bytes. | |
| Corpo da Solicitação - size: 105 bytes. | |
| Cabeçalho de Resposta | |

| | |
|---|---|
| - size: 257 bytes. | |
| Corpo de Resposta - size: 43 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/products |
| Método | POST |
| Parameter | |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 336 bytes. | |
| Corpo da Solicitação - size: 206 bytes. | |
| Cabeçalho de Resposta - size: 256 bytes. | |
| Corpo de Resposta - size: 95 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/payment/toggle |
| Método | PUT |
| Parameter | |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: | |

| | |
|---|---|
| 288 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 214 bytes. | |
| Corpo de Resposta - size: 33 bytes. | |
| Instances | 12 |
| Solution | Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security. |
| Reference | https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html<br>https://owasp.org/www-community/Security_Headers<br>https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security<br>https://caniuse.com/stricttransportsecurity<br>https://datatracker.ietf.org/doc/html/rfc6797 |
| Marcadores (Tags) | OWASP_2021_A05<br>OWASP_2017_A06<br>CWE-319 |
| CWE Id | 319 |
| WASC Id | 15 |
| Plugin Id | 10035 |

| **Baixo** | **X-Content-Type-Options Header Missing** |
|---|---|
| Descrição | The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing. |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | x-content-type-options |
| Ataque | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: | |

| | |
|---|---|
| 284 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 249 bytes. | |
| Corpo de Resposta - size: 499 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers |
| Método | GET |
| Parameter | x-content-type-options |
| Ataque | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 283 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 245 bytes. | |
| Corpo de Resposta - size: 2 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/products |
| Método | GET |
| Parameter | x-content-type-options |
| Ataque | |

| | |
|---|---|
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 282 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 249 bytes. | |
| Corpo de Resposta - size: 494 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |
| Parameter | x-content-type-options |
| Ataque | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 331 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta | |

| | |
|---|---|
| - size: 177 bytes. | |
| Corpo de Resposta - size: 485 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |
| Parameter | x-content-type-options |
| Ataque | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 343 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 177 bytes. | |
| Corpo de Resposta - size: 289 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/payment/toggle |
| Método | PUT |
| Parameter | x-content-type-options |
| Ataque | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. |
| Show / hide Request | |

| | |
|---|---|
| and Response | |
| Cabeçalho de Solicitação - size: 288 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 214 bytes. | |
| Corpo de Resposta - size: 33 bytes. | |
| Instances | 6 |
| Solution | Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.<br><br>If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing. |
| Reference | https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)<br>https://owasp.org/www-community/Security_Headers |
| Marcadores (Tags) | CWE-693<br>OWASP_2021_A05<br>OWASP_2017_A06 |
| CWE Id | 693 |
| WASC Id | 15 |
| Plugin Id | 10021 |

| **Informativo** | **Re-examine Cache-control Directives** |
|---|---|
| Descrição | The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached. |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | cache-control |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |

| | |
|---|---|
| Cabeçalho de Solicitação - size: 284 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 249 bytes. | |
| Corpo de Resposta - size: 499 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers |
| Método | GET |
| Parameter | cache-control |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 283 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 245 bytes. | |
| Corpo de Resposta - size: 2 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/products |
| Método | GET |
| Parameter | cache-control |

| | |
|---|---|
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 282 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 249 bytes. | |
| Corpo de Resposta - size: 494 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |
| Parameter | cache-control |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 331 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 177 bytes. | |

| | |
|---|---|
| Corpo de Resposta - size: 485 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |
| Parameter | cache-control |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 343 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 177 bytes. | |
| Corpo de Resposta - size: 289 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/payment/toggle |
| Método | PUT |
| Parameter | cache-control |
| Ataque | |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 288 bytes. | |

| | |
|---|---|
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 214 bytes. | |
| Corpo de Resposta - size: 33 bytes. | |
| Instances | 6 |
| Solution | For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable". |
| Reference | https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching<br>https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control<br>https://grayduck.mn/2021/09/13/cache-control-recommendations/ |
| Marcadores (Tags) | WSTG-v42-ATHN-06<br>CWE-525 |
| CWE Id | 525 |
| WASC Id | 13 |
| Plugin Id | 10015 |

| **Informativo** | **User Agent Fuzzer** |
|---|---|
| Descrição | Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response. |
| | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 254 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de | |

| | |
|---|---|
| Resposta - size: 252 bytes. | |
| Corpo de Resposta - size: 43.655 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 254 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 252 bytes. | |
| Corpo de Resposta - size: 43.655 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de | |

| | |
|---|---|
| Solicitação - size: 254 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 252 bytes. | |
| Corpo de Resposta - size: 43.655 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 266 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 252 bytes. | |
| Corpo de Resposta - size: 43.655 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | Cabeçalho do Agente de Usuário |

| | |
|---|---|
| Ataque | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0 |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 332 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 252 bytes. | |
| Corpo de Resposta - size: 43.655 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36 |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 319 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: | |

| | |
|---|---|
| 252 bytes. | |
| Corpo de Resposta - size: 43.655 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0 |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 282 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 252 bytes. | |
| Corpo de Resposta - size: 43.655 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: | |

| | |
|---|---|
| 276 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 252 bytes. | |
| Corpo de Resposta - size: 43.655 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 287 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 252 bytes. | |
| Corpo de Resposta - size: 43.655 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4 |
| Evidence | |

| | |
|---|---|
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 340 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 252 bytes. | |
| Corpo de Resposta - size: 43.655 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16 |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 345 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 252 bytes. | |
| Corpo de Resposta - size: | |

| | |
|---|---|
| 43.655 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/categories |
| Método | GET |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | msnbot/1.1 (+http://search.msn.com/msnbot.htm) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 250 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 252 bytes. | |
| Corpo de Resposta - size: 43.655 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 301 bytes. | |
| Corpo da Solicitaçã | |

| | |
|---|---|
| o - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 178 bytes. | |
| Corpo de Resposta - size: 26 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 301 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 26 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |

| | |
|---|---|
| Cabeçalho de Solicitação - size: 301 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 26 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 313 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 26 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |

| | |
|---|---|
| Ataque | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0 |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 379 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 26 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36 |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 366 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |

| | |
|---|---|
| Corpo de Resposta - size: 26 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0 |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 329 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 26 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 323 bytes. | |
| Corpo da Solicitaçã | |

| | |
|---|---|
| o - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 26 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 334 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 26 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4 |
| Evidence | |
| Other Info | |
| Show / hide Request | |

| | |
|---|---|
| and Response | |
| Cabeçalho de Solicitação - size: 387 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 26 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16 |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 392 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 26 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/auth |
| Método | POST |

| | |
|---|---|
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | msnbot/1.1 (+http://search.msn.com/msnbot.htm) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 297 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 26 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 313 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: | |

| | |
|---|---|
| 178 bytes. | |
| Corpo de Resposta - size: 45 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 313 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 45 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 313 bytes. | |

| | |
|---|---|
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 45 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 325 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 45 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0 |
| Evidence | |
| Other Info | |
| Show / hide | |

| | |
|---|---|
| Request and Response | |
| Cabeçalho de Solicitação - size: 391 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 45 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36 |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 378 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 45 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |

| | |
|---|---|
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0 |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 341 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 45 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 335 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: | |

| | |
|---|---|
| 183 bytes. | |
| Corpo de Resposta - size: 45 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 346 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 45 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4 |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: | |

| | |
|---|---|
| 399 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 45 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16 |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 404 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 45 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/customers/delete |
| Método | POST |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | msnbot/1.1 (+http://search.msn.com/msnbot.htm) |
| Evidence | |
| Other Info | |

| | |
|---|---|
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 309 bytes. | |
| Corpo da Solicitação - size: 28 bytes. | |
| Cabeçalho de Resposta - size: 183 bytes. | |
| Corpo de Resposta - size: 45 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/payment/toggle |
| Método | PUT |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 277 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 214 bytes. | |
| Corpo de Resposta - size: 33 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/payment/toggle |

| | |
|---|---|
| Método | PUT |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 289 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 214 bytes. | |
| Corpo de Resposta - size: 33 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/payment/toggle |
| Método | PUT |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36 |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 342 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta | |

| | |
|---|---|
| - size: 214 bytes. | |
| Corpo de Resposta - size: 33 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/payment/toggle |
| Método | PUT |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 299 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 214 bytes. | |
| Corpo de Resposta - size: 33 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/payment/toggle |
| Método | PUT |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp) |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: | |

| | |
|---|---|
| 310 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 214 bytes. | |
| Corpo de Resposta - size: 33 bytes. | |
| URL | https://i8z10k6wma.execute-api.us-east-1.amazonaws.com/lanchonete/payment/toggle |
| Método | PUT |
| Parameter | Cabeçalho do Agente de Usuário |
| Ataque | Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4 |
| Evidence | |
| Other Info | |
| Show / hide Request and Response | |
| Cabeçalho de Solicitação - size: 363 bytes. | |
| Corpo da Solicitação - size: 0 bytes. | |
| Cabeçalho de Resposta - size: 214 bytes. | |
| Corpo de Resposta - size: 33 bytes. | |
| Instances | 42 |
| Solution | |
| Reference | https://owasp.org/wstg |
| Marcadores (Tags) | |
| CWE Id | |
| WASC Id | |
| Plugin Id | 10104 |