Relatório de digitalização ZAP

Gerado com ZAP no ter. 19 mar. 2024, às 13:12:56

Versão ZAP: 2.14.0

ZAP é apoiado pela Crash Override Open Source Fellowship

Conteúdo

Sobre este relatório

Descrição do relatório

Webhook Snackhubpay via Ultrahook - antes

Parâmetros de relatório

Contextos

Nenhum contexto foi selecionado, portanto todos os contextos foram incluídos por padrão.

Locais

Os seguintes sites foram incluídos:

- `https://snackhubpay-mercadopago.ultrahook.com`

(Se nenhum site for selecionado, todos os sites serão incluídos por padrão.)

Um site incluído também deve estar dentro de um dos contextos incluídos para que seus dados sejam incluídos no relatório.

Níveis de risco

Incluído : Alto , Médio , Baixo , Informativo

Excluído : Nenhum

Níveis de confiança

Incluso : Usuário Confirmado , Alto , Médio , Baixo , Falso Positivo

Excluído : Nenhum

Resumos

Contagens de alertas por risco e confiança

Esta tabela mostra o número de alertas para cada nível de risco e confiança incluídos no relatório.

(As porcentagens entre colchetes representam a contagem como porcentagem do número total de alertas incluídos no relatório, arredondado para uma casa decimal.)

		Confiança					
		Usuário confirmado	alto	Médio	baixo	Falso Positivo	Total
Risco	alto	0 (0,0%)	0 (0,0%)	0 (0,0%)	1 (12,5%)	0 (0,0%)	1 (12,5%)
	Médio	0 (0,0%)	1 (12,5%)	1 (12,5%)	1 (12,5%)	0 (0,0%)	3 (37,5%)
	baixo	0 (0,0%)	2 (25,0%)	1 (12,5%)	0 (0,0%)	0 (0,0%)	3 (37,5%)

	Confiança					
	Usuário confirmado	alto	Médio	baixo	Falso Positivo	Total
Informativo	0 (0,0%)	0 (0,0%)	0 (0,0%)	1 (12,5%)	0 (0,0%)	1 (12,5%)
Total	0 (0,0%)	3 (37,5%)	2 (25,0%)	3 (37,5%)	0 (0,0%)	8 (100%)

Contagens de alertas por site e risco

Esta tabela mostra, para cada local para o qual foram gerados um ou mais alertas, o número de alertas gerados em cada nível de risco.

Alertas com nível de confiança de "Falso Positivo" foram excluídos dessas contagens.

(Os números entre parênteses são o número de alertas emitidos para o local nesse nível de risco ou acima dele.)

		Risco			
		Alto (= alto)	Médio (>= Médio)	Baixo (>= Baixo)	Informativo (>= Informativo)
Site	https://snackhubpay-mercadopago.ultrahook.com	1 (1)	3 (4)	3 (7)	1 (8)

Contagens de alertas por tipo de alerta

Esta tabela mostra o número de alertas de cada tipo de alerta, juntamente com o nível de risco do tipo de alerta.

(As porcentagens entre colchetes representam cada contagem como uma porcentagem, arredondada para uma casa decimal, do número total de alertas incluídos neste relatório.)

Tipo de alerta	Risco	Contar
Metadados de nuvem potencialmente expostos	alto	1 (12,5%)
Cabeçalho da Política de Segurança de Conteúdo (CSP) não definido	Médio	5 (62,5%)
Arquivo oculto encontrado	Médio	4 (50,0%)
Cabeçalho anti-clickjacking ausente	Médio	5 (62,5%)
Servidor vaza informações de versão por meio do campo de cabeçalho de resposta HTTP “Servidor”	baixo	5 (62,5%)
Cabeçalho Strict-Transport-Security não definido	baixo	5 (62,5%)
Cabeçalho X-Content-Type-Options ausente	baixo	5 (62,5%)
Reexamine as diretivas de controle de cache	Informativo	4 (50,0%)
Total		8

Alertas

Risco = Alto , Confiança = Baixo (1)

https://snackhubpay-mercadopago.ultrahook.com (1)

Metadados de nuvem potencialmente expostos (1)

▼ OBTENHA https://snackhubpay-mercadopago.ultrahook.com/latest/meta-data/

Etiquetas de alerta	▪ OWASP_2021_A05 ▪ OWASP_2017_A06
Descrição do alerta	O Cloud Metadata Attack tenta abusar de um servidor NGINX mal configurado para acessar os metadados da instância mantidos por provedores de serviços em nuvem como AWS, GCP e Azure. Todos esses provedores fornecem metadados por meio de um endereço IP interno não roteável '169.254.169.254' - isso pode ser exposto por servidores NGINX configurados incorretamente e acessado usando esse endereço IP no campo de cabeçalho do host.
Outras informações	Com base no código de status da resposta bem-sucedida, os metadados da nuvem podem ter sido retornados na resposta. Verifique os dados de resposta para ver se algum metadado da nuvem foi retornado. Os metadados retornados podem incluir informações que permitiriam a um invasor comprometer completamente o sistema.

Solicitar

▼ Linha de solicitação e seção de cabeçalho (271 bytes)

```
GET https://snackhubpay-mercadopago.ultrahook.com/latest/meta-data/ HTTP/1.1
host: 169.254.169.254
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Corpo da solicitação (0 bytes)

Resposta

▼ Linha de status e seção de cabeçalho (162 bytes)

```
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Tue, 19 Mar 2024 16:10:44 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 942
Connection: keep-alive
```

▼ Corpo de resposta (942 bytes)

```
  <!DOCTYPE html>
  <html>
    <head>
      <style type="text/css">
      body {
        font-family: 'Segoe UI', helvetica, arial, sans-serif;
      }
      </style>
```

```
    </head>
    <body>
      <h1>Trying to access your dev
environment?</h1>
      <p>What UltraHook does:</p>
      <ul>
        <li>Make it easy to receive
webhooks on localhost</li>
        <li>Relay HTTP POST
requests</li>
        <li>Provide a persistent
hostname</li>
        <li>Work through most
firewalls and run on most
computers</li>
        <li>Return a 200 OK status
code on HTTP POST requests</li>
      </ul>
      <p>What UltraHook does
<strong>not</strong> do:</p>
        <ul>
          <li>Expose your dev
environment to the world</li>
          <li>Relay HTTP GET
requests (this is why you see this
message)</li>
          <li>Relay the response
code from localhost back out to the
original requestor</li>
        </ul>
      </p>
    </body>
  </html>
```

Ataque 169.254.169.254

Solução Não confie em nenhum dado do usuário nas configurações do NGINX. Neste caso, é provavelmente o uso da variável $host, que está definido no cabeçalho

'Host' e pode ser controlado por um invasor.

Risco = Médio , Confiança = Alto (1)

https://snackhubpay-mercadopago.ultrahook.com (1)

Cabeçalho da Política de Segurança de Conteúdo (CSP) não definido (1)

▼ OBTENHA https://snackhubpay-mercadopago.ultrahook.com

Etiquetas de alerta
- OWASP_2021_A05
- OWASP_2017_A06

Descrição do alerta
A Política de Segurança de Conteúdo (CSP) é uma camada adicional de segurança que ajuda a detectar e mitigar certos tipos de ataques, incluindo Cross Site Scripting (XSS) e ataques de injeção de dados. Esses ataques são usados para tudo, desde roubo de dados até destruição de sites ou distribuição de malware. O CSP fornece um conjunto de cabeçalhos HTTP padrão que permitem aos proprietários de sites declarar fontes aprovadas de conteúdo que os navegadores devem ter permissão para carregar naquela página - os tipos cobertos são JavaScript, CSS, quadros HTML, fontes, imagens e objetos incorporáveis, como miniaplicativos Java, ActiveX, arquivos de áudio e vídeo.

Solicitar
▼ Linha de solicitação e seção de cabeçalho (275 bytes)

```
GET https://snackhubpay-
mercadopago.ultrahook.com HTTP/1.1
host: snackhubpay-
mercadopago.ultrahook.com
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/116.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Corpo da solicitação (0 bytes)

Resposta

▼ Linha de status e seção de cabeçalho (162 bytes)

```
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Tue, 19 Mar 2024 16:10:13 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 942
Connection: keep-alive
```

▼ Corpo de resposta (942 bytes)

```
  <!DOCTYPE html>
  <html>
    <head>
      <style type="text/css">
      body {
        font-family: 'Segoe UI',
helvetica, arial, sans-serif;
      }
      </style>
    </head>
    <body>
      <h1>Trying to access your dev
```

```
environment?</h1>
      <p>What UltraHook does:</p>
      <ul>
        <li>Make it easy to receive
webhooks on localhost</li>
        <li>Relay HTTP POST
requests</li>
        <li>Provide a persistent
hostname</li>
        <li>Work through most firewalls
and run on most computers</li>
        <li>Return a 200 OK status code
on HTTP POST requests</li>
      </ul>
      <p>What UltraHook does
<strong>not</strong> do:</p>
        <ul>
          <li>Expose your dev
environment to the world</li>
          <li>Relay HTTP GET requests
(this is why you see this message)</li>
          <li>Relay the response code
from localhost back out to the original
requestor</li>
        </ul>
      </p>
    </body>
  </html>
```

Solução Certifique-se de que seu servidor web, servidor de aplicativos, balanceador de carga, etc. esteja configurado para definir o cabeçalho Content-Security-Policy.

Risco = Médio , Confiança = Médio (1)

https://snackhubpay-mercadopago.ultrahook.com (1)

Cabeçalho anti-clickjacking ausente (1)

▼ OBTENHA https://snackhubpay-mercadopago.ultrahook.com

Etiquetas de alerta

- OWASP_2021_A05
- WSTG-v42-CLNT-09
- OWASP_2017_A06

Descrição do alerta

A resposta não inclui Content-Security-Policy com diretiva 'frame-ancestors' ou X-Frame-Options para proteção contra ataques de 'ClickJacking'.

Solicitar

▼ Linha de solicitação e seção de cabeçalho (275 bytes)

```
GET https://snackhubpay-
mercadopago.ultrahook.com HTTP/1.1
host: snackhubpay-
mercadopago.ultrahook.com
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/116.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Corpo da solicitação (0 bytes)

Resposta

▼ Linha de status e seção de cabeçalho (162 bytes)

```
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Tue, 19 Mar 2024 16:10:13 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 942
```

```
Connection: keep-alive
```

▼ Corpo de resposta (942 bytes)

```
  <!DOCTYPE html>
  <html>
    <head>
      <style type="text/css">
      body {
        font-family: 'Segoe UI',
helvetica, arial, sans-serif;
      }
      </style>
    </head>
    <body>
      <h1>Trying to access your dev
environment?</h1>
      <p>What UltraHook does:</p>
      <ul>
        <li>Make it easy to receive
webhooks on localhost</li>
        <li>Relay HTTP POST
requests</li>
        <li>Provide a persistent
hostname</li>
        <li>Work through most
firewalls and run on most
computers</li>
        <li>Return a 200 OK status
code on HTTP POST requests</li>
      </ul>
      <p>What UltraHook does
<strong>not</strong> do:</p>
        <ul>
          <li>Expose your dev
environment to the world</li>
          <li>Relay HTTP GET requests
(this is why you see this message)</li>
          <li>Relay the response code
```

```
from localhost back out to the
original requestor</li>
        </ul>
      </p>
    </body>
  </html>
```

Parâmetro x-frame-options

Solução Os navegadores da Web modernos suportam os cabeçalhos HTTP Content-Security-Policy e X-Frame-Options. Certifique-se de que um deles esteja definido em todas as páginas da web retornadas pelo seu site/aplicativo.

Se você espera que a página seja enquadrada apenas pelas páginas do seu servidor (por exemplo, faz parte de um FRAMESET), então você desejará usar SAMEORIGIN; caso contrário, se você nunca espera que a página seja enquadrada, você deverá usar DENY. Como alternativa, considere implementar a diretiva "frame-ancestors" da Política de Segurança de Conteúdo.

Risco = Médio , Confiança = Baixo (1)

https://snackhubpay-mercadopago.ultrahook.com (1)

Arquivo oculto encontrado (1)

▼ OBTENHA https://snackhubpay-mercadopago.ultrahook.com/.hg

Etiquetas de alerta
- OWASP_2021_A05
- WSTG-v42-CONF-05

- OWASP_2017_A06

Descrição do alerta

Um arquivo confidencial foi identificado como acessível ou disponível. Isso pode vazar informações administrativas, de configuração ou de credenciais que podem ser aproveitadas por um indivíduo mal-intencionado para atacar ainda mais o sistema ou conduzir esforços de engenharia social.

Solicitar

▼ Linha de solicitação e seção de cabeçalho (279 bytes)

```
GET https://snackhubpay-mercadopago.ultrahook.com/.hg HTTP/1.1
host: snackhubpay-mercadopago.ultrahook.com
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Corpo da solicitação (0 bytes)

Resposta

▼ Linha de status e seção de cabeçalho (162 bytes)

```
HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Tue, 19 Mar 2024 16:10:50 GMT
Content-Type: text/html;charset=utf-8
Content-Length: 942
Connection: keep-alive
```

▼ Corpo de resposta (942 bytes)

```
<!DOCTYPE html>
<html>
  <head>
    <style type="text/css">
    body {
      font-family: 'Segoe UI',
helvetica, arial, sans-serif;
    }
    </style>
  </head>
  <body>
    <h1>Trying to access your dev
environment?</h1>
    <p>What UltraHook does:</p>
    <ul>
      <li>Make it easy to receive
webhooks on localhost</li>
      <li>Relay HTTP POST
requests</li>
      <li>Provide a persistent
hostname</li>
      <li>Work through most firewalls
and run on most computers</li>
      <li>Return a 200 OK status code
on HTTP POST requests</li>
    </ul>
    <p>What UltraHook does
<strong>not</strong> do:</p>
      <ul>
        <li>Expose your dev
environment to the world</li>
        <li>Relay HTTP GET requests
(this is why you see this message)</li>
        <li>Relay the response code
from localhost back out to the original
requestor</li>
      </ul>
    </p>
```

```
    </body>
</html>
```

Evidência	HTTP/1.1 200 OK
Solução	Considere se o componente é realmente necessário ou não na produção; se não for, desative-o. Se for, garanta que o acesso a ele exija autenticação e autorização apropriadas ou limite a exposição a sistemas internos ou IPs de origem específicos, etc.

Risco = Baixo , Confiança = Alto (2)

https://snackhubpay-mercadopago.ultrahook.com (2)

Servidor vaza informações de versão por meio do campo de cabeçalho de resposta HTTP "Servidor" (1)

▶ OBTENHA https://snackhubpay-mercadopago.ultrahook.com

Cabeçalho Strict-Transport-Security não definido (1)

▶ OBTENHA https://snackhubpay-mercadopago.ultrahook.com

Risco = Baixo , Confiança = Médio (1)

https://snackhubpay-mercadopago.ultrahook.com (1)

Cabeçalho X-Content-Type-Options ausente (1)

▶ OBTENHA https://snackhubpay-mercadopago.ultrahook.com

Risco = Informativo , Confiança = Baixo (1)

https://snackhubpay-mercadopago.ultrahook.com (1)

Reexamine as diretivas de controle de cache (1)

▶ OBTENHA https://snackhubpay-mercadopago.ultrahook.com

Apêndice

Tipos de alerta

Esta seção contém informações adicionais sobre os tipos de alertas no relatório.

Metadados de nuvem potencialmente expostos

Fonte	gerado por um scanner ativo (Metadados de nuvem potencialmente exposta)
Referência	▪ https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/

Cabeçalho da Política de Segurança de Conteúdo (CSP) não definido

Fonte	gerado por um scanner passivo (Content Security Policy (CSP) Header Not Set)
ID do CWE	693
ID WASC	15
Referência	▪ https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content

_Security_Policy

- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- http://www.w3.org/TR/CSP/
- http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html
- http://www.html5rocks.com/en/tutorials/security/content-security-policy/
- http://caniuse.com/#feat=contentsecuritypolicy
- http://content-security-policy.com/

Arquivo oculto encontrado

Fonte	gerado por um scanner ativo (Hidden File Finder)
ID do CWE	538
ID WASC	13
Referência	• https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html

Cabeçalho anti-clickjacking ausente

Fonte	gerado por um scanner passivo (cabeçalho anti-clickjacking)

ID do CWE	1021
ID WASC	15
Referência	▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Servidor vaza informações de versão por meio do campo de cabeçalho de resposta HTTP "Servidor"

Fonte	gerado por um scanner passivo (HTTP Server Response Header)
ID do CWE	200
ID WASC	13
Referência	▪ http://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 ▪ http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx ▪ http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

Cabeçalho Strict-Transport-Security não definido

Fonte	gerado por um scanner passivo (Strict-Transport-Security Header)
ID do CWE	319

ID WASC	15
Referência	▪ https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html ▪ https://owasp.org/www-community/Security_Headers ▪ http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security ▪ http://caniuse.com/stricttransportsecurity ▪ http://tools.ietf.org/html/rfc6797

Cabeçalho X-Content-Type-Options ausente

Fonte	gerado por um scanner passivo (X-Content-Type-Options Header Missing)
ID do CWE	693
ID WASC	15
Referência	▪ http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx ▪ https://owasp.org/www-community/Security_Headers

Reexamine as diretivas de controle de cache

Fonte	gerado por um scanner passivo (Reexaminar diretivas de controle de cache)

ID do CWE	525
ID WASC	13
Referência	▪ https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching ▪ https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control ▪ https://grayduck.mn/2021/09/13/cache-control-recommendations/