Relatório de digitalização ZAP

Gerado com ZAP no ter. 19 mar. 2024, às 10:49:27

Versão ZAP: 2.14.0

ZAP é apoiado pela Crash Override Open Source Fellowship

Conteúdo

Sobre este relatório

Descrição do relatório

Snackhubpay

Parâmetros de relatório

Contextos

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

Locais

Os seguintes sites foram incluídos:

- http://localhost:8090

(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%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
	Médio	0 (0,0%)	1 (11,1%)	1 (11,1%)	0 (0,0%)	0 (0,0%)	2 (22,2%)
	baixo	0 (0,0%)	0 (0,0%)	3 (33,3%)	1 (11,1%)	0 (0,0%)	4 (44,4%)
	Informativo	0 (0,0%)	0 (0,0%)	2 (22,2%)	1 (11,1%)	0 (0,0%)	3 (33,3%)

	Confiança				
	Usuário confirmado	alto	Médio	baixo	Falso Positivo	Total
Total	0 (0,0%)	1 (11,1%)	6 (66,7%)	2 (22,2%)	0 (0,0%)	9 (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	http://localhost:809 0	0 (0)	2 (2)	3 (5)	3 (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

Tipo de alerta	Risco	Contar
Cabeçalho da Política de Segurança de Conteúdo (CSP) não definido	Médio	3 (33,3%)
Cabeçalho anti-clickjacking ausente	Médio	1 (11,1%)
Divulgação de erro de aplicativo	baixo	2 (22,2%)
Divulgação de Dados e Hora - Unix	baixo	76 (844,4%)
Divulgação de informações - Mensagens de Erro de Depuração	baixo	1 (11,1%)
Cabeçalho X-Content-Type-Options ausente	baixo	8 (88,9%)
Divulgação de Informações - Comentários Suspeitos	Informativo	2 (22,2%)
Aplicativo Web moderno	Informativo	1 (11,1%)
Fuzzer do agente do usuário	Informativo	96 (1.066,7%)
Total		9

Alertas

Risco = Médio , Confiança = Alto (1)

http://localhost:8090 (1)

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

▼ OBTER

http://localhost:8090/mp/orders/createOrderQrCode/1589696702/SNACKBARPOTESTSELLER/qrs

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 (733 bytes) GET http://localhost:8090/mp/orders/createOrderQrCode/1589696702/SNACKBARPOTESTSELLER/qrs HTTP/1.1 host: localhost:8090 Proxy-Connection: keep-alive sec-ch-ua: "Chromium";v="122", "Not(A:Brand";v="24", "Google Chrome";v="122"

```
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/122.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,applicat
ion/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Language: pt-BR,pt;q=0.9,en-
US;q=0.8,en;q=0.7
```

▼ Corpo da solicitação (0 bytes)

Resposta

▼ Linha de status e seção de cabeçalho (158 bytes)

```
HTTP/1.1 500 Internal Server Error
Connection: keep-alive
Content-Type: text/html;charset=UTF-8
Content-Length: 52
Date: Tue, 19 Mar 2024 13:22:44 GMT
```

▼ Corpo de resposta (52 bytes)

```
Ocorreu um erro interno, tente
novamente mais tarde.
```

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)

http://localhost:8090 (1)

Cabeçalho anti-clickjacking ausente (1)

▶ OBTER http://localhost:8090/swagger-ui/index.html

Risco = Baixo , Confiança = Médio (3)

http://localhost:8090 (3)

Divulgação de erro de aplicativo (1)

▼ OBTER
http://localhost:8090/mp/orders/createOrderQrCode/1589696702/SNACKBARPOTESTSELLER/qrs

Etiquetas de alerta
- WSTG-v42-ERRH-02
- WSTG-v42-ERRH-01
- OWASP_2021_A05
- OWASP_2017_A06

Descrição do alerta
Esta página contém uma mensagem de erro/aviso que pode revelar informações confidenciais, como a localização do arquivo que produziu a exceção não tratada. Essas informações podem ser usadas para lançar novos ataques contra a aplicação web. O alerta pode ser um falso positivo se a mensagem de erro for

encontrada dentro de uma página de documentação.

Solicitar

▼ Linha de solicitação e seção de cabeçalho (733 bytes)

```
GET
http://localhost:8090/mp/orders/createOr
derQrCode/1589696702/SNACKBARPOTESTSELLE
R/qrs HTTP/1.1
host: localhost:8090
Proxy-Connection: keep-alive
sec-ch-ua: "Chromium";v="122",
"Not(A:Brand";v="24", "Google
Chrome";v="122"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/122.0.0.0
Safari/537.36
Accept:
text/html,application/xhtml+xml,applicat
ion/xml;q=0.9,image/avif,image/webp,imag
e/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Language: pt-BR,pt;q=0.9,en-
US;q=0.8,en;q=0.7
```

▼ Corpo da solicitação (0 bytes)

Resposta

▼ Linha de status e seção de cabeçalho (158 bytes)

```
HTTP/1.1 500 Internal Server Error
Connection: keep-alive
Content-Type: text/html;charset=UTF-8
Content-Length: 52
Date: Tue, 19 Mar 2024 13:22:44 GMT
```

▼ Corpo de resposta (52 bytes)

```
Ocorreu um erro interno, tente
novamente mais tarde.
```

Evidência	`HTTP/1.1 500 Internal Server Error`
Solução	Revise o código-fonte desta página. Implemente páginas de erro personalizadas. Considere implementar um mecanismo para fornecer uma referência/identificador de erro exclusivo ao cliente (navegador) enquanto registra os detalhes no lado do servidor e não os expõe ao usuário.

Divulgação de informações - Mensagens de Erro de Depuração (1)

▶ OBTER http://localhost:8090/v3/api-docs

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

▶ OBTER http://localhost:8090/swagger-ui/index.css

Risco = Baixo , Confiança = Baixo (1)

Risco = Informativo , Confiança = Médio (2)

http://localhost:8090 (2)

Aplicativo Web moderno (1)

▶ OBTER http://localhost:8090/swagger-ui/index.html

Fuzzer do agente do usuário (1)

▶ OBTER http://localhost:8090/comerciante

Risco = Informativo , Confiança = Baixo (1)

http://localhost:8090 (1)

Divulgação de Informações - Comentários Suspeitos (1)

▶ OBTER http://localhost:8090/swagger-ui/swagger-ui-standalone-preset.js

Apêndice

Tipos de alerta

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

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/

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

Divulgação de erro de aplicativo

Fonte	gerado por um scanner passivo (revelação de erro de aplicativo)
ID do CWE	200
ID WASC	13

Divulgação de Dados e Hora - Unix

Fonte	levantado por um scanner passivo (Divulgação de Dados e Hora)
ID do CWE	200
ID WASC	13
Referência	▪ http://projects.webappsec.org/w/page/13246936/Information%20Leakage

Divulgação de informações - Mensagens de Erro de Depuração

Fonte	levantada por um scanner passivo (Divulgação de informações - Mensagens de Erro de Depuração)
ID do CWE	200
ID WASC	13

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

Divulgação de Informações - Comentários Suspeitos

Fonte	levantado por um scanner passivo (Divulgação de Informações - Comentários Suspeitos)
ID do CWE	200
ID WASC	13

Aplicativo Web moderno

Fonte	gerado por um scanner passivo (Modern Web Application)

Fuzzer do agente do usuário

Fonte	gerado por um scanner ativo (User Agent Fuzzer)
Referência	▪ https://owasp.org/wstg