Relatório de digitalização ZAP

Gerado com ZAP em seg. 8 jul. 2024, às 12:48:32

Versão ZAP: 2.15.0

O ZAP é apoiado pela Crash Override Open Source Fellowship

Conteúdo

Sobre este relatório

Parâmetros do relatório

Contextos

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

Sítios

Os seguintes sites foram incluídos:

- `http://hostlocal`

(Se nenhum site foi selecionado, todos os sites foram 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

Inclui : `Alto` , `Médio` , `Baixo` , `Informativo`

Excluído : Nenhum

Níveis de confiança

Incluído : `Usuário Confirmado` , `Alto` , `Médio` , `Baixo`

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

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 parênteses representam a contagem como uma porcentagem do número total de alertas incluídos no relatório, arredondado para uma casa decimal.)

		Confiança				
		Usuário confirmado	Alto	Médio	Baixo	Total
Risco	Alto	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)	0 (0,0%)
	Médio	0 (0,0%)	2 (14,3%)	1 (7,1%)	2 (14,3%)	5 (35,7%)
	Baixo	0 (0,0%)	1 (7,1%)	4 (28,6%)	0 (0,0%)	5 (35,7%)
	Informativo	0 (0,0%)	0 (0,0%)	3 (21,4%)	1 (7,1%)	4 (28,6%)
	Total	0 (0,0%)	3 (21,4%)	8 (57,1%)	3 (21,4%)	14 (100%)

Contagens de alertas por local e risco

Esta tabela mostra, para cada site para o qual um ou mais alertas foram gerados, 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 gerados para o site nesse nível de risco ou acima dele.)

	Risco			
	Alto (= Alto)	**Médio (>= Médio)**	**Baixo (>= Baixo)**	**Informativo (>= Informativo)**
http://hostlocal Site	0 (0)	5 (5)	5 (10)	4 (14)

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 parênteses representam cada contagem como uma porcentagem, arredondada para uma casa decimal, do número total de alertas incluídos neste relatório.)

Tipo de alerta	Risco	Contar
Adulteração de parâmetros	Médio	2 (14,3%)
Ausência de tokens Anti-CSRF	Médio	3 (21,4%)
Cabeçalho da Política de Segurança de Conteúdo (CSP) não definido	Médio	6 (42,9%)
Arquivo oculto encontrado	Médio	2 (14,3%)
Total		14

Tipo de alerta	Risco	Contar
Cabeçalho anti-clickjacking ausente	Médio	4 (28,6%)
Cookie sem sinalizador HttpOnly	Baixo	2 (14,3%)
Cookie sem atributo SameSite	Baixo	2 (14,3%)
O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By"	Baixo	5 (35,7%)
Vazamentos de informações de versão do servidor por meio do campo de cabeçalho de resposta HTTP "Servidor"	Baixo	8 (57,1%)
Cabeçalho X-Content-Type-Options ausente	Baixo	5 (35,7%)
Cookie com Escopo Fraco	Informativo	4 (28,6%)
Aplicação Web Moderna	Informativo	1 (7,1%)
Resposta de gerenciamento de sessão identificada	Informativo	5 (35,7%)
Fuzzer do agente do usuário	Informativo	24 (171,4%)
Total		14

Alertas

Risco = Médio , Confiança = Alto (2)

http://localhost (2)

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

▶ OBTER http://localhost/robots.txt

Arquivo Oculto Encontrado (1)

▶ OBTER http://localhost/status-do-servidor

Risco = Médio , Confiança = Médio (1)

http://localhost (1)

Cabeçalho anti-clickjacking ausente (1)

▶ OBTER http://localhost/backupUP/

Risco = Médio , Confiança = Baixo (2)

http://localhost (2)

Adulteração de parâmetros (1)

▶ POSTAR http://localhost/backupUP/login.php

Ausência de tokens Anti-CSRF (1)

▶ OBTER http://localhost/backupUP/register.php

Risco = Baixo , Confiança = Alto (1)

http://localhost (1)

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

▶ OBTER http://localhost/robots.txt

Risco = Baixo , Confiança = Médio (4)

http://localhost (4)

Cookie sem sinalizador HttpOnly (1)

▶ OBTER http://localhost/backupUP/register.php

Cookie sem atributo SameSite (1)

▶ OBTER http://localhost/backupUP/register.php

O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By" (1)

▶ OBTER http://localhost/backupUP/

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

▶ OBTER http://localhost/backupUP/

Risco = Informativo , Confiança = Médio (3)

http://localhost (3)

Aplicação Web Moderna (1)

▶ OBTER http://localhost/backupUP/register.php

Resposta de gerenciamento de sessão identificada (1)

▶ OBTER http://localhost/backupUP/register.php

Fuzzer do agente do usuário (1)

▶ POSTAR http://localhost/backupUP/register.php

Risco = Informativo , Confiança = Baixo (1)

http://localhost (1)

Cookie com Escopo Fraco (1)

▶ OBTER http://localhost/backupUP/register.php

Apêndice

Tipos de alerta

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

Adulteração de parâmetros

Fonte	levantado por um scanner ativo (Adulteração de parâmetros)
Identificação do CWE	472
Identificação do WASC	20

Ausência de tokens Anti-CSRF

Fonte	levantado por um scanner passivo (Ausência de tokens Anti-CSRF)
Identificação do CWE	352

Identificação do WASC	9
Referência	▪ https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html ▪ https://cwe.mitre.org/data/definitions/352.html

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

Fonte	gerado por um scanner passivo (Cabeçalho da Política de Segurança de Conteúdo (CSP) Não Definido)
Identificação do CWE	693
Identificação do 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 ▪ https://www.w3.org/TR/CSP/ ▪ https://w3c.github.io/webappsec-csp/ ▪ https://web.dev/articles/csp

- https://caniuse.com/#feat=contentsecuritypolicy
- https://content-security-policy.com/

Arquivo oculto encontrado

Fonte	levantado por um scanner ativo (Hidden File Finder)
Identificação do CWE	538
Identificação do WASC	13
Referência	- https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html - https://httpd.apache.org/docs/current/mod/mod_status.html

Cabeçalho anti-clickjacking ausente

Fonte	levantado por um scanner passivo (Cabeçalho Anti-clickjacking)
Identificação do CWE	1021
Identificação do WASC	15
Referência	- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

Cookie sem sinalizador HttpOnly

Fonte	gerado por um scanner passivo (Cookie No HttpOnly Flag)
Identificação do CWE	1004
Identificação do WASC	13
Referência	▪ https://owasp.org/www-community/HttpOnly

Cookie sem atributo SameSite

Fonte	gerado por um scanner passivo (Cookie sem Atributo SameSite)
Identificação do CWE	1275
Identificação do WASC	13
Referência	▪ https://tools.ietf.org/html/draft-ietf-httpbis-cookie-mesmo-site

O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By"

Fonte	levantado por um scanner passivo (O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By")
Identificação do CWE	200
Identificação do WASC	13

Referência	▪ https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework ▪ https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

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

Fonte	gerado por um scanner passivo (cabeçalho de resposta do servidor HTTP)
Identificação do CWE	200
Identificação do WASC	13
Referência	▪ https://httpd.apache.org/docs/current/mod/core.html#servertokens ▪ https://learn.microsoft.com/en-us/previous-versions/msp-np/ff648552(v=pandp.10) ▪ https://www.troyhunt.com/shhh-dont-let-your-response-headers/

Cabeçalho X-Content-Type-Options ausente

Fonte	gerado por um scanner passivo (X-Content-Type-Options Header Missing)
Identificação do CWE	693

Identificação do WASC	15
Referência	▪ https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) ▪ https://owasp.org/www-community/Security_Headers

Cookie com Escopo Fraco

Fonte	levantado por um scanner passivo (Cookie com Escopo Fraco)
Identificação do CWE	565
Identificação do WASC	15
Referência	▪ https://tools.ietf.org/html/rfc6265#section-4.1 ▪ https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html ▪ https://code.google.com/p/browsersec/wiki/Part2#Política_de_mesma_origem_para_cookies

Aplicação Web Moderna

Fonte	gerado por um scanner passivo (Aplicação Web Moderna)

Resposta de gerenciamento de sessão identificada

Fonte	gerado por um scanner passivo (Session Management Response Identified)
Referência	▪ https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id

Fuzzer do agente do usuário

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