ZAP by Checkmarx Scanning Report

Sites: https://www.google-analytics.com https://axeptio-api.goadopt.io https://ad.doubleclick.net https://www.facebook.com https://adservice.google.com https://static.hotjar.com https://15560714.fls.doubleclick.net https://static.doubleclick.net https://play.google.com https://cdn.denomatic.com https://jnn-pa.googleapis.com https://googleads.g.doubleclick.net https://app-3qnu8i2v1y.marketingautomation.services https://analytics.google.com https://koi-3qnu8i2v1y.marketingautomation.services https://www.googletagmanager.com https://www.google.com.br https://tag.goadopt.io https://carmelhoteis.com.br https://www.google.com

Generated on sáb., 20 set. 2025 17:28:44

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Nível de Risco	Number of Alerts
Alto	0
Médio	5
Baixo	8
Informativo	7

Alertas

Nome	Nível de Risco	Number of Instances
Ausência de tokens Anti-CSRF	Médio	2
Configuração Incorreta Entre Domínios	Médio	13
Content Security Policy (CSP) Header Not Set	Médio	4
Missing Anti-clickjacking Header	Médio	3
Session ID in URL Rewrite	Médio	3
Cookie No HttpOnly Flag	Baixo	1
Cookie with SameSite Attribute None	Baixo	1
Cross-Domain JavaScript Source File Inclusion	Baixo	5
Divulgação de Data e Hora - Unix	Baixo	45
O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By"	Baixo	2

Server Leaks Version Information via "Server" HTTP Response Header Field	Baixo	4
Strict-Transport-Security Header Not Set	Baixo	20
X-Content-Type-Options Header Missing	Baixo	11
Cookie com Escopo Fraco	Informativo	1
Divulgação de Informações - Comentários Suspeitos	Informativo	14
Information Disclosure - Sensitive Information in URL	Informativo	1
Modern Web Application	Informativo	1
Re-examine Cache-control Directives	Informativo	4
Retrieved from Cache	Informativo	3
Session Management Response Identified	Informativo	1

Alert Detail

Médio	Ausência de tokens Anti-CSRF
Descrição	Não foram localizados tokens Anti-CSRF no formulário de submissão HTML. Uma falsificação de solicitação entre sites (Cross-Site Request Forgery ou simplesmente CSRF) é um ataque que envolve forçar a vítima a enviar uma solicitação HTTP a um destino alvo sem seu conhecimento ou intenção, a fim de realizar uma ação como a vítima. A causa implícita é a funcionalidade do aplicativo usando ações previsíveis em URLs /formulários, de maneira repetível. A natureza do ataque é que o CSRF explora a confiança que um site tem em um usuário. Em contrapartida, um ataque do tipo Cross-Site Scripting (XSS) explora a confiança que um usuário tem em um site. Como o XSS, os ataques CSRF não são necessariamente entre sites, mas também podem ser. A falsificação de solicitação entre sites também é conhecida por "CSRF", "XSRF", "one-click attack", "session riding", "confused deputy", e "sea surf". Os ataques CSRF são efetivos em várias situações, incluindo: * - A vítima tem uma sessão ativa no site de destino; * - A vítima está autenticada por meio de autenticação HTTP no site de destino; * - A vítima está na mesma rede local do site de destino. O CSRF era usado principalmente para executar ações contra um site-alvo usando os privilégios da vítima, mas técnicas recentes foram descobertas para vazamento de informações obtendo acesso às respostas. O risco de vazamento/divulgação não autorizada de informações aumenta drasticamente quando o site de destino é vulnerável a XSS, porque o XSS pode ser usado como uma plataforma para CSRF, permitindo que o ataque opere dentro dos limites da política de mesma origem.
URL	https://app-3qnu8i2v1y.marketingautomation.services/prospector/form/MzawMLE0NTMwBQA/MzQ2MU42SUzVTTUySdM1MbY01bVINU7RNU1NTk5KM081MUtMAQA?rf__sb=https%3A%2F%2Fcarmelhoteis.com.br%2F&agentreferrer__sb=https%3A%2F%2Fcarmelhoteis.com.br%2F&_tk=202509%7C68cf0a4304006702a43af8de&instance=ux2jtr
Método	GET
Ataque	
Evidence	<form method="post" action="/prospector/thanks/MzawMLE0NTMwBQA/1343c4ae-e24f-4395-8e3d-5eccbf7e46ad" id="form_1343c4ae-e24f-4395-8e3d-5eccbf7e46ad" enctype="multipart/form-data">

Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] foi encontrado nos seguintes formulários HTML: [Form 1: "4684102658-6" "accountid__sb" "agentreferrer__sb" "companyprofileid__sb" "defaultCampaignID" "field_4628333570_input" "field_4628334594_input" "field_4628335618_input" "formid__sb" "trackingid__sb"].
URL	https://carmelhoteis.com.br/
Método	GET
Ataque	
Evidence	<form id="motor-reserva" method="post" action="javascript: goconsulta()">
Other Info	Nenhum token Anti-CSRF conhecido [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] foi encontrado nos seguintes formulários HTML: [Form 1: "data-chegada" "data-partida" "enviar"].
Instances	2
Solution	Fase: Arquitetura e Design. 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. Por exemplo, use pacotes anti-CSRF, como o OWASP CSRFGuard. Fase: Implementação. Certifique-se de que seu aplicativo esteja livre de problemas de cross-site scripting (XSS), porque a maioria das defesas CSRF pode ser contornada usando script controlado por invasor. Fase: Arquitetura e Design. Gere um número arbitrário de uso único e exclusivo (ou Nonce = "N" de "number" - número em inglês - e "once" de "uma vez" também em inglês) para cada formulário, coloque o nonce no formulário e verifique-o ao receber o formulário. Certifique-se de que o nonce não seja previsível (CWE-330). Observe que isso pode ser contornado usando XSS. Identifique operações especialmente perigosas. Quando o usuário realizar uma operação perigosa, envie uma solicitação de confirmação separada para garantir que o usuário pretendia realizar aquela operação. Observe que isso pode ser contornado usando XSS. Utilize o controle ESAPI Session Management. Este controle inclui um componente para CSRF. Não use o método GET para qualquer solicitação que acione uma mudança de estado. Fase: Implementação. Verifique o cabeçalho HTTP Referer para ver se a solicitação foi originada de uma página esperada. Isso pode interromper funcionalidades legítimas, porque os usuários ou proxies podem ter desativado o envio do Referer por motivos de privacidade.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Médio	Configuração Incorreta Entre Domínios
Descrição	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.
URL	https://app-3qnu8i2v1y.marketingautomation.services/prospector/getFormData/MzawMLE0NTMwBQA/1343c4ae-e24f-4395-8e3d-5eccbf7e46ad?rf__sb=https%253A%252F%252Fcarmelhoteis.com.br%252F&agentreferrer__sb=https%253A%252F%252Fcarmelhoteis.com.br%252F&_tk=202509%7C68cf0a4304006702a43af8de&instance=ux2jtr&rf__doc=https%3A%2F%2Fcarmelhoteis.com.br%2F
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://static.doubleclick.net/instream/ad_status.js
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://static.hotjar.com/c/hotjar-5082103.js?sv=7
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://static.hotjar.com/c/hotjar-5082146.js?sv=7
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://static.hotjar.com/c/hotjar-5082148.js?sv=7

Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://tag.goadopt.io/injector.js/v2/0017?website_code=04f3aae2-99c2-4f51-81ae-95070b7ea85f
Método	GET
Ataque	
Evidence	access-control-allow-origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://tag.goadopt.io/injector.js?website_code=04f3aae2-99c2-4f51-81ae-95070b7ea85f
Método	GET
Ataque	
Evidence	access-control-allow-origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://www.googletagmanager.com/gtag/js?id=AW-17102942276&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão

	disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://www.googletagmanager.com/gtag/js?id=DC-15560714&l=denoCsDataLayer
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
URL	https://www.googletagmanager.com/gtm.js?id=GTM-5VFVP9L
Método	GET
Ataque	
Evidence	Access-Control-Allow-Origin: *
Other Info	A configuração incorreta do CORS no servidor da web permite solicitações de leitura entre domínios de domínios arbitrários de terceiros, usando APIs não autenticadas neste domínio. No entanto, as implementações do navegador da Web não permitem que terceiros arbitrários leiam a resposta de APIs autenticadas. Isso reduz o risco um pouco. Essa configuração incorreta pode ser usada por um invasor para acessar dados que estão disponíveis de maneira não autenticada, mas que usam alguma outra forma de segurança, como lista de permissões de endereços IP.
Instances	13
Solution	Certifique-se de que dados confidenciais não estejam disponíveis de maneira não autenticada (usando uma lista branca/de permissões de endereços IP, por exemplo). Configure o cabeçalho HTTP "Access-Control-Allow-Origin" para um conjunto mais restritivo de domínios ou remova todos os cabeçalhos CORS inteiramente, para permitir que o navegador web aplique a Same Origin Policy (SOP) de uma maneira mais restritiva.
	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.

Reference	html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14
Plugin Id	10098

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 cer data injection attacks. These attacks are used for everything from data theft to site defacement headers that allow website owners to declare approved sources of content that browsers should JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, A
URL	https://15560714.fls.doubleclick.net/activityi;src=15560714;type=visit0;cat=visit0;ord=91877040 u27=counter;pscdl=noapi;frm=0;_tu=IFA;gtm=45fe59h0v9223939777za200zd9223939777xec;g tag_exp=101509157~103116026~103200004~103233427~104527906~104528501~10468420 epver=2;dc_random=SqAdXtJrlDH4BXFKbT2NZSyYsbuyFmc_Nw;_dc_test=1;~oref=https%3A
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://app-3qnu8i2v1y.marketingautomation.services/prospector/form/MzawMLE0NTMwBQA /MzQ2MU42SUzVTTUySdM1MbY01bVINU7RNU1NTk5KM081MUtMAQA?rf__sb=https%3A% 2F%2Fcarmelhoteis.com.br%2F&_tk=202509%7C68cf0a4304006702a43af8de&instance=ux2jt
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://carmelhoteis.com.br/
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://jnn-pa.googleapis.com/$rpc/google.internal.waa.v1.Waa/Create
Método	OPTIONS
Ataque	
Evidence	
Other Info	
Instances	4
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Cont
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Poli 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/
CWE Id	693

WASC Id	15
Plugin Id	10038

Médio	Missing Anti-clickjacking Header
Descrição	The response does not protect against 'ClickJacking' attacks. It should include either Content-S Options.
URL	https://15560714.fls.doubleclick.net/activityi;src=15560714;type=visit0;cat=visit0;ord=91877040 u27=counter;pscdl=noapi;frm=0;_tu=IFA;gtm=45fe59h0v9223939777za200zd9223939777xec;g tag_exp=101509157~103116026~103200004~103233427~104527906~104528501~10468420 epver=2;dc_random=SqAdXtJrlDH4BXFKbT2NZSyYsbuyFmc_Nw;_dc_test=1;~oref=https%3A
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://app-3qnu8i2v1y.marketingautomation.services/prospector/form/MzawMLE0NTMwBQA /MzQ2MU42SUzVTTUySdM1MbY01bVINU7RNU1NTk5KM081MUtMAQA?rf__sb=https%3A%2 2F%2Fcarmelhoteis.com.br%2F&_tk=202509%7C68cf0a4304006702a43af8de&instance=ux2jt
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://carmelhoteis.com.br/
Método	GET
Ataque	
Evidence	
Other Info	
Instances	3
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP header site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET expect the page to be framed, you should use DENY. Alternatively consider implementing Cont
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Médio	Session ID in URL Rewrite
Descrição	URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site ref
URL	https://analytics.google.com/g/collect?v=2&tid=G-B0LW80ZCN3&gtm=45be59h0v9116860628z us&sr=1920x1080&ir=1&frm=0&pscdl=noapi&ec_mode=a&_eu=EAAAAAQ&_s=1&tag_exp=10 A9is&en=page_view&tfd=2185
Método	POST
Ataque	
Evidence	1758399043
Other	

Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-B0LW80ZCN3&gtm=45je59h0h1v911686062&us=1920x1080&ir=1&frm=0&pscdl=noapi&_eu=EAAIAAQ&_s=2&tag_exp=101509157~103A9is&_tu=CA&en=user_engagement&_et=20257&tfd=443150
Método	POST
Ataque	
Evidence	1758399043
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-JDLGW1172L&gtm=45je59g1h2v91190&us=1920x1080&ir=1&frm=0&pscdl=noapi&_eu=EAAAAAQ&_s=1&tag_exp=101509157~1033A%2F%2Fwww.zaproxy.org%2Fdownload%2F&dr=https%3A%2F%2Fwww.zaproxy.org%2Fd
Método	POST
Ataque	
Evidence	1758400030
Other Info	
Instances	3
Solution	For secure content, put session ID in a cookie. To be even more secure consider using a combi
Reference	https://seclists.org/webappsec/2002/q4/111
CWE Id	598
WASC Id	13
Plugin Id	3

Baixo	**Cookie No HttpOnly Flag**
Descrição	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	https://koi-3qnu8i2v1y.marketingautomation.services/koi?rf=&hn=carmelhoteis.com.br&lg=en-US&sr=1920x1080&cd=24&vr=2.4.1&se=1758399043254&tk=202509%7C68cf0a4304006702a43af8de&ac=KOI-4KR91Q9G7C&ts=1758399955&pt=NaN&pl=NaN&loc=https%3A%2F%2Fcarmelhoteis.com.br%2F&tp=page&ti=Carmel%20Hot%C3%A9is
Método	GET
Ataque	
Evidence	Set-Cookie: koitk
Other Info	
Instances	1
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Baixo	**Cookie with SameSite Attribute None**

Descrição	A cookie has been set with its SameSite attribute set to "none", which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://koi-3qnu8i2v1y.marketingautomation.services/koi?rf=&hn=carmelhoteis.com.br&lg=en-US&sr=1920x1080&cd=24&vr=2.4.1&se=1758399043254&tk=202509%7C68cf0a4304006702a43af8de&ac=KOI-4KR91Q9G7C&ts=1758399955&pt=NaN&pl=NaN&loc=https%3A%2F%2Fcarmelhoteis.com.br%2F&tp=page&ti=Carmel%20Hot%C3%A9is
Método	GET
Ataque	
Evidence	Set-Cookie: koitk
Other Info	
Instances	1
Solution	Certifique-se de que o atributo SameSite esteja definido como 'lax' ou, de preferência, 'strict' para todos os cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Baixo	**Cross-Domain JavaScript Source File Inclusion**
Descrição	The page includes one or more script files from a third-party domain.
URL	https://carmelhoteis.com.br/
Método	GET
Ataque	
Evidence	<script src="//tag.goadopt.io/injector.js?website_code=04f3aae2-99c2-4f51-81ae-95070b7ea85f" class="adopt-injector"></script>
Other Info	
URL	https://carmelhoteis.com.br/
Método	GET
Ataque	
Evidence	<script id="script-infochat" src='https://cdn.asksuite.com/infochat.js?dataConfig=https://control.asksuite.com/api/companies/carmel-whatsapp-corporativo'></script>
Other Info	
URL	https://carmelhoteis.com.br/
Método	GET
Ataque	
Evidence	<script type="text/javascript" src="https://code.jquery.com/jquery-3.4.1.min.js"></script>
Other Info	
URL	https://carmelhoteis.com.br/
Método	GET
Ataque	

Evidence	<script type="text/javascript" src="https://koi-3QNU8I2V1Y.marketingautomation.services/client/form.js?ver=2.0.1"></script>
Other Info	
URL	https://carmelhoteis.com.br/
Método	GET
Ataque	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=UA-58552173-1"></script>
Other Info	
Instances	5
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

Baixo	**Divulgação de Data e Hora - Unix**
Descrição	A timestamp was disclosed by the application/web server. - Unix
URL	https://app-3qnu8i2v1y.marketingautomation.services/prospector/form/MzawMLE0NTMwBQA/M
Método	GET
Ataque	
Evidence	1463593986
Other Info	1463593986, which evaluates to: 2016-05-18 14:53:06.
URL	https://app-3qnu8i2v1y.marketingautomation.services/prospector/getFormData/MzawMLE0NTM
Método	GET
Ataque	
Evidence	1463593986
Other Info	1463593986, which evaluates to: 2016-05-18 14:53:06.
URL	https://googleads.g.doubleclick.net/pagead/viewthroughconversion/16564907894/?random=175 config&gtm=45be59h0v9116860628z8847111689za200zb847111689zd847111689xec&gcd=13 com&npa=0&pscdl=noapi&auid=757426853.1758399043&data=event%3Dgtag.config&rfmt=3&
Método	GET
Ataque	
Evidence	1758399043
Other Info	1758399043, which evaluates to: 2025-09-20 17:10:43.
URL	https://googleads.g.doubleclick.net/pagead/viewthroughconversion/17102942276/?random=175 config&gtm=45be59h0v9220701822z8847111689za200zb847111689zd847111689xec&gcd=13 com&npa=0&pscdl=noapi&auid=757426853.1758399043&data=event%3Dgtag.config&rfmt=3&
Método	GET
Ataque	
Evidence	1758399043

Other Info	1758399043, which evaluates to: 2025-09-20 17:10:43.
URL	https://googleads.g.doubleclick.net/pagead/viewthroughconversion/17102942276/?random=175 config&gtm=45be59h0v9220701822z8847111689za200zb847111689zd847111689xec&gcd=1 googleadservices.com&npa=0&pscdl=noapi&auid=757426853.1758399043&data=event%3Dgt
Método	GET
Ataque	
Evidence	1758399043
Other Info	1758399043, which evaluates to: 2025-09-20 17:10:43.
URL	https://www.google.com/pagead/1p-conversion/17102942276/?random=1758399955021&cv=11&fst=1758399955021&bg=ffffff&guid=ON&async=1&en=purch 3A%2F%2Fcarmelhoteis.com.br%2F&label=L4q8CNGg-8saEMTgqNs_&frm=0&tiba=Carmel%2
Método	GET
Ataque	
Evidence	1758399043
Other Info	1758399043, which evaluates to: 2025-09-20 17:10:43.
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1508970993
Other Info	1508970993, which evaluates to: 2017-10-25 20:36:33.
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1537002063
Other Info	1537002063, which evaluates to: 2018-09-15 06:01:03.
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1541459225
Other Info	1541459225, which evaluates to: 2018-11-05 21:07:05.
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1555081692
Other Info	1555081692, which evaluates to: 2019-04-12 12:08:12.
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	

Evidence	1695183700
Other Info	1695183700, which evaluates to: 2023-09-20 01:21:40.
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1747873779
Other Info	1747873779, which evaluates to: 2025-05-21 21:29:39.
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1779033703
Other Info	1779033703, which evaluates to: 2026-05-17 13:01:43.
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1899447441
Other Info	1899447441, which evaluates to: 2030-03-11 05:17:21.
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1925078388
Other Info	1925078388, which evaluates to: 2031-01-01 20:59:48.
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1955562222
Other Info	1955562222, which evaluates to: 2031-12-20 16:43:42.
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1986661051
Other Info	1986661051, which evaluates to: 2032-12-14 15:17:31.
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1996064986
Other	

Info	1996064986, which evaluates to: 2033-04-02 11:29:46.
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	2024104815
Other Info	2024104815, which evaluates to: 2034-02-21 00:20:15.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1508970993
Other Info	1508970993, which evaluates to: 2017-10-25 20:36:33.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1537002063
Other Info	1537002063, which evaluates to: 2018-09-15 06:01:03.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1541459225
Other Info	1541459225, which evaluates to: 2018-11-05 21:07:05.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1555081692
Other Info	1555081692, which evaluates to: 2019-04-12 12:08:12.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1695183700
Other Info	1695183700, which evaluates to: 2023-09-20 01:21:40.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1747873779
Other Info	1747873779, which evaluates to: 2025-05-21 21:29:39.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0

Método	GET
Ataque	
Evidence	1779033703
Other Info	1779033703, which evaluates to: 2026-05-17 13:01:43.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1899447441
Other Info	1899447441, which evaluates to: 2030-03-11 05:17:21.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1925078388
Other Info	1925078388, which evaluates to: 2031-01-01 20:59:48.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1955562222
Other Info	1955562222, which evaluates to: 2031-12-20 16:43:42.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1986661051
Other Info	1986661051, which evaluates to: 2032-12-14 15:17:31.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	1996064986
Other Info	1996064986, which evaluates to: 2033-04-02 11:29:46.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	2024104815
Other Info	2024104815, which evaluates to: 2034-02-21 00:20:15.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET

Ataque	
Evidence	1508970993
Other Info	1508970993, which evaluates to: 2017-10-25 20:36:33.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
Ataque	
Evidence	1537002063
Other Info	1537002063, which evaluates to: 2018-09-15 06:01:03.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
Ataque	
Evidence	1541459225
Other Info	1541459225, which evaluates to: 2018-11-05 21:07:05.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
Ataque	
Evidence	1555081692
Other Info	1555081692, which evaluates to: 2019-04-12 12:08:12.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
Ataque	
Evidence	1695183700
Other Info	1695183700, which evaluates to: 2023-09-20 01:21:40.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
Ataque	
Evidence	1747873779
Other Info	1747873779, which evaluates to: 2025-05-21 21:29:39.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
Ataque	
Evidence	1779033703
Other Info	1779033703, which evaluates to: 2026-05-17 13:01:43.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
Ataque	
Evidence	1899447441

Other Info	1899447441, which evaluates to: 2030-03-11 05:17:21.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
Ataque	
Evidence	1925078388
Other Info	1925078388, which evaluates to: 2031-01-01 20:59:48.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
Ataque	
Evidence	1955562222
Other Info	1955562222, which evaluates to: 2031-12-20 16:43:42.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
Ataque	
Evidence	1986661051
Other Info	1986661051, which evaluates to: 2032-12-14 15:17:31.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
Ataque	
Evidence	1996064986
Other Info	1996064986, which evaluates to: 2033-04-02 11:29:46.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
Ataque	
Evidence	2024104815
Other Info	2024104815, which evaluates to: 2034-02-21 00:20:15.
Instances	45
Solution	Confirme manualmente se os dados do carimbo de data/hora não são confidenciais e se os dad
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

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://tag.goadopt.io/injector.js/v2/0017?website_code=04f3aae2-99c2-4f51-81ae-95070b7ea85f
Método	GET
Ataque	
Evidence	x-powered-by: Express
Other Info	
URL	https://tag.goadopt.io/injector.js?website_code=04f3aae2-99c2-4f51-81ae-95070b7ea85f
Método	GET
Ataque	
Evidence	x-powered-by: Express
Other Info	
Instances	2
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 https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	497
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 head
URL	https://analytics.google.com/g/collect?v=2&tid=G-B0LW80ZCN3&gtm=45be59h0v9116860628z&us&sr=1920x1080&ir=1&frm=0&pscdl=noapi&ec_mode=a&_eu=EAAAAAQ&_s=1&tag_exp=10A9is&en=page_view&tfd=2185
Método	POST
Ataque	
Evidence	Golfe2
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-B0LW80ZCN3&gtm=45je59h0h1v9116860628&us&sr=1920x1080&ir=1&frm=0&pscdl=noapi&_eu=EAAIAAQ&_s=2&tag_exp=101509157~1031A9is&_tu=CA&en=user_engagement&_et=20257&tfd=443150
Método	POST
Ataque	
Evidence	Golfe2
Other Info	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-JDLGW1172L&gtm=45je59g1h2v91190&us&sr=1920x1080&ir=1&frm=0&pscdl=noapi&_eu=EAAAAAQ&_s=1&tag_exp=101509157~1033A%2F%2Fwww.zaproxy.org%2Fdownload%2F&dr=https%3A%2F%2Fwww.zaproxy.org%2Fd
Método	POST
Ataque	
Evidence	Golfe2

Other Info	
URL	https://www.google.com/ccm/collect?en=page_view&dl=https%3A%2F%2Fcarmelhoteis.com.br 1758399043&navt=n&npa=0&gtm=45He59h0v847111689za200zd847111689xea&gcd=13l3l3l3
Método	POST
Ataque	
Evidence	scaffolding on HTTPServer2
Other Info	
Instances	4
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress th
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
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 serv
URL	https://app-3qnu8i2v1y.marketingautomation.services/prospector/form/MzawMLE0NTMwBQA/M
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://app-3qnu8i2v1y.marketingautomation.services/prospector/getFormData/MzawMLE0NTM
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://carmelhoteis.com.br/
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://carmelhoteis.com.br/wp-content/uploads/2020/10/homecarmelshort.mp4
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://cdn.denomatic.com/drs/610-bc123253bdb3.js
Método	GET

Ataque	
Evidence	
Other Info	
URL	https://googleads.g.doubleclick.net/pagead/id
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://googleads.g.doubleclick.net/pagead/viewthroughconversion/16564907894/?random=175 config&gtm=45be59h0v9116860628z8847111689za200zb847111689zd847111689xec&gcd=13 com&npa=0&pscdl=noapi&auid=757426853.1758399043&data=event%3Dgtag.config&rfmt=3&
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://googleads.g.doubleclick.net/pagead/viewthroughconversion/17102942276/?random=175 config&gtm=45be59h0v9220701822z8847111689za200zb847111689zd847111689xec&gcd=13 com&npa=0&pscdl=noapi&auid=757426853.1758399043&data=event%3Dgtag.config&rfmt=3&
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://googleads.g.doubleclick.net/pagead/viewthroughconversion/17102942276/?random=175 config&gtm=45be59h0v9220701822z8847111689za200zb847111689zd847111689xec&gcd=13 googleadservices.com&npa=0&pscdl=noapi&auid=757426853.1758399043&data=event%3Dgt
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://koi-3qnu8i2v1y.marketingautomation.services/koi?rf=&hn=carmelhoteis.com.br&lg=en-U
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://static.doubleclick.net/instream/ad_status.js
Método	GET
Ataque	
Evidence	
Other Info	

URL	https://tag.goadopt.io/injector.js/v2/0017?website_code=04f3aae2-99c2-4f51-81ae-95070b7ea8
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://www.google.com/pagead/1p-conversion/17102942276/?random=1758399955021&cv=11&fst=1758399955021&bg=ffffff&guid=ON&async=1&en=purcha 3A%2F%2Fcarmelhoteis.com.br%2F&label=L4q8CNGg-8saEMTgqNs_&frm=0&tiba=Carmel%2
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://jnn-pa.googleapis.com/$rpc/google.internal.waa.v1.Waa/Create
Método	OPTIONS
Ataque	
Evidence	
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-B0LW80ZCN3&gtm=45be59h0v9116860628z us&sr=1920x1080&ir=1&frm=0&pscdl=noapi&ec_mode=a&_eu=EAAAAAQ&_s=1&tag_exp=10
Método	POST
Ataque	
Evidence	
Other Info	
URL	https://analytics.google.com/g/collect?v=2&tid=G-B0LW80ZCN3&gtm=45je59h0h1v9116860628 us&sr=1920x1080&ir=1&frm=0&pscdl=noapi&_eu=EAAIAAQ&_s=2&tag_exp=101509157~1031
Método	POST
Ataque	
Evidence	
Other Info	
URL	https://axeptio-api.goadopt.io/flow
Método	POST
Ataque	
Evidence	
Other Info	
URL	https://play.google.com/log?hasfast=true&authuser=0&format=json
Método	POST
Ataque	
Evidence	
Other Info	

URL	https://www.google-analytics.com/g/collect?v=2&tid=G-JDLGW1172L&gtm=45je59g1h2v91190 us&sr=1920x1080&ir=1&frm=0&pscdl=noapi&_eu=EAAAAAQ&_s=1&tag_exp=101509157~103 2F&dr=https%3A%2F%2Fwww.zaproxy.org%2Fdownload%2F&dt=ZAP%20%E2%80%93%20[
Método	POST
Ataque	
Evidence	
Other Info	
URL	https://www.google.com/ccm/collect?en=page_view&dl=https%3A%2F%2Fcarmelhoteis.com.br 1758399043&navt=n&npa=0&gtm=45He59h0v847111689za200zd847111689xea&gcd=13l3l3l3
Método	POST
Ataque	
Evidence	
Other Info	
Instances	20
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Stri
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
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://app-3qnu8i2v1y.marketingautomation.services/prospector/form /MzawMLE0NTMwBQA /MzQ2MU42SUzVTTUySdM1MbY01bVINU7RNU1NTk5KM081MUtMAQA?rf__sb=https% 3A%2F%2Fcarmelhoteis.com.br%2F&agentreferrer__sb=https%3A%2F%2Fcarmelhoteis. com.br%2F&_tk=202509%7C68cf0a4304006702a43af8de&instance=ux2jtr
Método	GET
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.
URL	https://app-3qnu8i2v1y.marketingautomation.services/prospector/getFormData /MzawMLE0NTMwBQA/1343c4ae-e24f-4395-8e3d-5eccbf7e46ad?rf__sb=https%253A% 252F%252Fcarmelhoteis.com.br%252F&agentreferrer__sb=https%253A%252F% 252Fcarmelhoteis.com.br%252F&_tk=202509% 7C68cf0a4304006702a43af8de&instance=ux2jtr&rf__doc=https%3A%2F%2Fcarmelhoteis. com.br%2F
Método	GET

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.
URL	https://carmelhoteis.com.br/
Método	GET
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.
URL	https://carmelhoteis.com.br/wp-content/uploads/2020/10/homecarmelshort.mp4
Método	GET
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.
URL	https://cdn.denomatic.com/drs/610-bc123253bdb3.js
Método	GET
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.
URL	https://koi-3qnu8i2v1y.marketingautomation.services/koi?rf=&hn=carmelhoteis.com.br&lg=en-US&sr=1920x1080&cd=24&vr=2.4.1&se=1758399043254&tk=202509%7C68cf0a4304006702a43af8de&ac=KOI-4KR91Q9G7C&ts=1758399955&pt=NaN&pl=NaN&loc=https%3A%2F%2Fcarmelhoteis.com.br%2F&tp=page&ti=Carmel%20Hot%C3%A9is
Método	GET
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.
URL	https://www.google.com/complete/search?client=firefox&channel=ftr&q=
Método	GET
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.

URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
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.
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
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.
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
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.
URL	https://play.google.com/log?hasfast=true&authuser=0&format=json
Método	POST
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.
Instances	11
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. 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) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informativo	**Cookie com Escopo Fraco**
	Os cookies podem ser atribuídos por domínio ou caminho. Essa verificação se refere apenas ao escopo do domínio. O escopo do domínio aplicado a um cookie determina quais domínios podem acessá-lo. Por exemplo, um cookie pode ter seu escopo definido estritamente para um subdomínio, por exemplo, www.naoconfiavel.com.br, ou vagamente

Descrição	para um domínio pai, por exemplo, naoconfiavel.com.br. No último caso, qualquer subdomínio de naoconfiavel.com.br pode acessar o cookie. Cookies de escopo mais fraco são comuns em megaaplicativos como google.com e live.com. Os cookies definidos a partir de um subdomínio como app.foo.bar são transmitidos apenas para esse domínio pelo navegador. No entanto, os cookies com escopo para um domínio de nível pai podem ser transmitidos ao pai ou a qualquer subdomínio do pai.
URL	https://koi-3qnu8i2v1y.marketingautomation.services/koi?rf=&hn=carmelhoteis.com.br&lg=en-US&sr=1920x1080&cd=24&vr=2.4.1&se=1758399043254&tk=202509%7C68cf0a4304006702a43af8de&ac=KOI-4KR91Q9G7C&ts=1758399955&pt=NaN&pl=NaN&loc=https%3A%2F%2Fcarmelhoteis.com.br%2F&tp=page&ti=Carmel%20Hot%C3%A9is
Método	GET
Ataque	
Evidence	
Other Info	The origin domain used for comparison was: koi-3qnu8i2v1y.marketingautomation.services koitk=202509%7C68cf0a4304006702a43af8de
Instances	1
Solution	Sempre defina o escopo dos cookies para FQDN (Fully Qualified Domain Name).
Reference	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#Same-origin_policy_for_cookies
CWE Id	565
WASC Id	15
Plugin Id	90033

Informativo	**Divulgação de Informações - Comentários Suspeitos**
Descrição	The response appears to contain suspicious comments which may help an attacker.
URL	https://app-3qnu8i2v1y.marketingautomation.services/prospector/form/MzawMLE0NTMwBQA/M7C68cf0a4304006702a43af8de&instance=ux2jtr
Método	GET
Ataque	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected in likely comment: "// This is a fix fo
URL	https://app-3qnu8i2v1y.marketingautomation.services/prospector/form/MzawMLE0NTMwBQA/M7C68cf0a4304006702a43af8de&instance=ux2jtr
Método	GET
Ataque	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "// the default f
URL	https://app-3qnu8i2v1y.marketingautomation.services/prospector/form/MzawMLE0NTMwBQA/M7C68cf0a4304006702a43af8de&instance=ux2jtr
Método	GET
Ataque	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in likely comment: "// use a sele

URL	https://carmelhoteis.com.br/
Método	GET
Ataque	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in likely comment: "//carmelhoteis
URL	https://carmelhoteis.com.br/
Método	GET
Ataque	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in likely comment: "//schema.org
URL	https://googleads.g.doubleclick.net/pagead/viewthroughconversion/16564907894/?random=175 config&gtm=45be59h0v9116860628z8847111689za200zb847111689zd847111689xec&gcd=13 2Fcarmelhoteis.com.br%2F&frm=0&tiba=Carmel%20Hot%C3%A9is&hn=www.googleadservice
Método	GET
Ataque	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//www.google.c
URL	https://googleads.g.doubleclick.net/pagead/viewthroughconversion/17102942276/?random=175 config&gtm=45be59h0v9220701822z8847111689za200zb847111689zd847111689xec&gcd=13 2Fcarmelhoteis.com.br%2F&frm=0&tiba=Carmel%20Hot%C3%A9is&hn=www.googleadservice
Método	GET
Ataque	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//www.google.c
URL	https://googleads.g.doubleclick.net/pagead/viewthroughconversion/17102942276/?random=175 config&gtm=45be59h0v9220701822z8847111689za200zb847111689zd847111689xec&gcd=13 3A%2F%2Fcarmelhoteis.com.br%2F&frm=0&tiba=Carmel%20Hot%C3%A9is&hn=www.google
Método	GET
Ataque	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//www.google.c
URL	https://static.hotjar.com/c/hotjar-5082103.js?sv=7
Método	GET
Ataque	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//metrics.hotjar
URL	https://static.hotjar.com/c/hotjar-5082146.js?sv=7
Método	GET
Ataque	
Evidence	user

Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//metrics.hotjar
URL	https://static.hotjar.com/c/hotjar-5082148.js?sv=7
Método	GET
Ataque	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//metrics.hotjar
URL	https://www.googletagmanager.com/gtag/js?id=AW-16564907894&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//")&&(a
URL	https://www.googletagmanager.com/gtag/js?id=G-B0LW80ZCN3&cx=c&gtm=4e59h0
Método	GET
Ataque	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in likely comment: "//")&&(a
URL	https://www.googletagmanager.com/gtag/js?id=UA-58552173-1
Método	GET
Ataque	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in likely comment: "//"+Fi(3)+"/de
Instances	14
Solution	Remova todos os comentários que retornam informações que podem ajudar um invasor e corrig
Reference	
CWE Id	615
WASC Id	13
Plugin Id	10027

Informativo	**Information Disclosure - Sensitive Information in URL**
Descrição	A solicitação parecia conter informações confidenciais vazadas no URL. Isso pode violar a PCI e a maioria das políticas de conformidade organizacional. Você pode configurar a lista de strings para esta verificação para adicionar ou remover valores específicos para seu ambiente.
URL	https://play.google.com/log?hasfast=true&authuser=0&format=json
Método	POST
Ataque	
Evidence	authuser
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: user authuser
Instances	1
Solution	Não passe informações confidenciais em URIs.

Reference	
CWE Id	598
WASC Id	13
Plugin Id	10024

Informativo	**Modern Web Application**
Descrição	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://app-3qnu8i2v1y.marketingautomation.services/prospector/form/MzawMLE0NTMwBQA/MzQ2MU42SUzVTTUySdM1MbY01bVINU7RNU1NTk5KM081MUtMAQA?rf__sb=https%3A%2F%2Fcarmelhoteis.com.br%2F&agentreferrer__sb=https%3A%2F%2Fcarmelhoteis.com.br%2F&_tk=202509%7C68cf0a4304006702a43af8de&instance=ux2jtr
Método	GET
Ataque	
	<script type="text/javascript"> var isPreview = 0; var baseURL = ''; var formDataURL = baseURL + '/prospector/getFormData/MzawMLE0NTMwBQA/1343c4ae-e24f-4395-8e3d-5eccbf7e46ad' + window.location.hash; var conditionGroupsRaw = {"conditionGroups":[]," formConditionalNodes":[{"deleteTimestamp":"0000-00-00 00:00:00","id":45060098," companyProfileID":308495605,"isRootNode":0,"companyFormFieldID":400000290852866," label":"Primeiro nome","children":[],"value":"Primeiro nome"},{"deleteTimestamp":"0000-00-00 00:00:00","id":45061122,"companyProfileID":308495605,"isRootNode":0," companyFormFieldID":400000290853890,"label":"Sobrenome","children":[],"value":" Sobrenome"},{"deleteTimestamp":"0000-00-00 00:00:00","id":45062146,"companyProfileID": 308495605,"isRootNode":0,"companyFormFieldID":400000290854914,"label":"E-mail"," children":[],"value":"E-mail"},{"deleteTimestamp":"0000-00-00 00:00:00","id":45063170," companyProfileID":308495605,"isRootNode":0,"companyFormFieldID":400000290856962," label":"Estado","children":[],"value":"Estado"},{"deleteTimestamp":"0000-00-00 00:00:00"," id":45064194,"companyProfileID":308495605,"isRootNode":0,"companyFormFieldID": 400000290857986,"label":"Pol\u00edtica de dados:","children":[],"value":"Pol\u00edtica de dados:"}]}; var hiddenFields = []; var commaSepStringContains = function commaSepStringContains(needle, haystack) { var safeNeedle = needle.replace(/[\-\[\]\/\{\}\(\)*\+\?\.\\\^\$|]/g, "\\$&"); var r = new RegExp('(^|, ?)' + safeNeedle + '(,|$)'); return typeof haystack == 'string' ? haystack.match(r) !== null : false; }; var getCookie = function getCookie(cookie_name) { if (cookie_name) { var results = document.cookie.match('(^|;) ?' + cookie_name + '=([^;]*)(;|$)'); if (results) { return (unescape(results[2])); } return null; } return document.cookie; } var getParams = function () { var vars = {}; var currentLocation = window.location.href; currentLocation.replace(location.hash, '').replace(/[?&]+([^=&]+)=?([^&]*)?/gi, // regexp function (m, key, value) { // callback vars[key] = value !== undefined ? value : ''; }); vars.rf__doc = document.referrer; return vars; }(); var parseFormData = function (apiData) { if (!apiData || !apiData.data) { return; } var jsonData = apiData.data; jsonData = typeof jsonData === 'object' && jsonData ? jsonData : {}; if (jsonData.campaignID) { $('input[name="defaultCampaignID"]').val(jsonData.campaignID); } else { $('input[name="defaultCampaignID"]').remove(); } if (getParams['redirectUrl']) { getParams['redirectUrl'] = decodeURIComponent(getParams['redirectUrl']); redirectURL = getParams['redirectUrl']; } if (jsonData.redirectUrl) { jsonData.redirectUrl = decodeURIComponent(jsonData.redirectUrl); // relative links needs to append base path if (jsonData.redirectUrl.match(/^\/[^\/].*$/)) { var parser = document.createElement('a'); parser.href = document.referrer; redirectURL = parser.protocol + '//' + parser.host + jsonData.redirectUrl; } else { redirectURL = jsonData.redirectUrl; } } var redirectHandlesPost = 0; if (redirectURL) { if (redirectHandlesPost) { $(formID).attr('action', redirectURL); $(formID).attr('target', '_top'); } else { $(formID).ajaxComplete(function (event, xhr, settings) { // the default form action has a redirect from .../save/... to .../thanks/... var ajaxUrl = settings.url.toLowerCase().replace('/save/', '/_/'); var formUrl = $(formID).prop('action').toLowerCase().replace('/thanks/', '/_/'); // Urls may have different formats in local vs prod, so just grab the part we care about ajaxUrl = ajaxUrl.substring(ajaxUrl.indexOf('prospector/_/')); formUrl = formUrl.substring(formUrl.indexOf('prospector/_/')); if (ajaxUrl === formUrl) { window.top.location = redirectURL; } }); } } if (jsonData.referrer) { // pass the `true referrer` for campaign attribution getParams['rf__doc'] = jsonData.referrer; } if (jsonData.agentReferrer) { $('input[name="agentreferrer__sb"]').val(jsonData.agentReferrer); } else { $('input[name="agentreferrer__sb"]').remove(); } // Get the first party tracking cookie var tk = getCookie('__ss_tk'); if ((!tk || tk == '_') && jsonData.trackingID && jsonData.trackingID != '_') { // The

Evidence	first party cookie was not set, use the third party cookie if available tk = jsonData.trackingID; } if (tk && tk !== '_') { $('input[name="trackingid__sb"]').val(tk); } else { $('input[name="trackingid__sb"]').remove(); } if (jsonData.accountID) { $('input[name="accountid__sb"]').val(jsonData.accountID); } else { $('input[name="accountid__sb"]').remove(); } // inject styles if (jsonData.cssURL) { jsonData.cssURL = decodeURIComponent(jsonData.cssURL); if (document.createStyleSheet) { document.createStyleSheet(jsonData.cssURL); } else { $('<link rel="stylesheet" type="text/css" href="' + jsonData.cssURL + '">').appendTo('head'); } } if (getParams['css_url']) { getParams['css_url'] = decodeURIComponent(getParams['css_url']); } if (jsonData.stylesheet) { $('<style>' + jsonData.stylesheet + '</style>').appendTo('head'); } var $input = null; var fieldID = 0; var movedGDPRToEnd = true; var setupLeadFields = function setupLeadFields(leadCache) { // Move GDPR to the last item in the list. if (!movedGDPRToEnd) { var $gdprConsentField = $('input[name^=\'gdprConsentField\']'); if ($gdprConsentField) { var $gdpr = $('#' + $gdprConsentField.val()); var $lastSibling = $gdpr.siblings(':last'); $gdpr.remove(); $gdpr.insertBefore($lastSibling); } movedGDPRToEnd = true; } var progressiveCount = 0; $('input.auto-filled, select.auto-filled, textarea.auto-filled').each(function() { var fieldName = $(this).attr('name').replace('[]', ''); fieldName = typeof fieldName === 'string' ? fieldName.trim() : fieldName; if (!leadCache[fieldName] || leadCache[fieldName] === 'undefined') { return; } var el = this; var vals; var $progressive = $('li.progressive').first(); var $list = $(this).closest('li'); var canReplace = !$(this).is('.progressive, .always-shown') && !$list.is('.hide'); // Progressive profiling queue if ($progressive.length && canReplace) { progressiveCount += 1; $list.addClass('hide'); $progressive .removeClass('progressive hide') .find('input').removeClass('progressive'); } if (el.type == 'select-one') { vals = leadCache[fieldName]; for (var o in el.options) { if (!el.options.hasOwnProperty(o)) { continue; } var option = el.options[o]; if (option.value && commaSepStringContains(option.value, vals)) { option.selected = true; } } } else if (el.type == 'checkbox' || el.type == 'radio') { vals = leadCache[fieldName]; if (el.value && commaSepStringContains(el.value, vals)) { el.checked = true; } } else if (!el.value || el.type === 'hidden') { el.value = leadCache[fieldName]; } // trigger change event so conditional-form-fields can process rules. $(el).change(); }); return progressiveCount; }; if (jsonData.leadCache) { var leadCache = jsonData.leadCache; var count = 0; $('input, select, textarea').each(function() { // remove any progressive fields that already have values var $el = $(this); var fieldName = $el.attr('name').replace('[]', ''); fieldName = typeof fieldName === 'string' ? fieldName.trim() : fieldName; var hasValue = Boolean(leadCache[fieldName]); if ($el.is('.progressive') && hasValue) { $el.closest('li').remove(); } }); do { count = setupLeadFields(leadCache); } while (count > 0); } $('li.hide .progressive').prop('disabled', true); $('.campaign_question').remove(); for (var f in formFields) { if (!formFields.hasOwnProperty(f)) { continue; } var field = formFields[f]; fieldName = 'field_' + field.fieldID; if (getParams[field.systemName] || getParams[fieldName]) { fieldID = '#' + fieldName; $(fieldID).remove(); } fieldName = 'ref_' + field.fieldID; if (getParams[fieldName]) { $('#' + fieldName).remove(); } } for (var p in getParams) { if (!getParams.hasOwnProperty(p)) { continue; } if (p.indexOf('_') !== 0 && !hiddenFields.includes(p)) { $input = $('<input>').attr({ type: 'hidden', name: p, value: getParams[p], }); $('.get_input_values').append($input); hiddenFields.push(p); } } if (jsonData.csrfToken) { $input = $('<input>').attr({ type: 'hidden', name: 'csrfToken', value: jsonData.csrfToken }); $('.get_input_values').append($input); } // Set up default values from the jsonData if (jsonData.formFields) { $.each(jsonData.formFields, function(f) { var field = jsonData.formFields[f]; fieldname = (field.isReferred === '1' ? 'ref_' : 'field_') + field.fieldID; if (field.defaultValue) { $('[name="' + fieldname + '"]').each(function () { if (!this.value) { this.value = field.defaultValue; // Trigger change event for conditional-form-fields $(this).change(); } }); } if (field.defaultPlaceholder && (getParams._usePlaceholders || isPreview)) { $('[name="' + fieldname + '"]').each(function () { this.placeholder = field.defaultPlaceholder; }); } }); } }; // If tracking ID comes in after form rendering, // add it to the form. function trackingIDBackup() { // attachEvent and detachEvent are for IE versions <=8 var eventMethod = window.addEventListener ? 'addEventListener' : 'attachEvent'; var removeEventMethod = window.removeEventListener ? 'removeEventListener' : 'detachEvent'; var eventer = window[eventMethod]; var removeEventer = window[removeEventMethod]; var messageEvent = (eventMethod === "attachEvent") ? "onmessage" : "message"; function onTrackingIDBackupMessageReceived(e) { var bodyNodeList = document.getElementsByClassName('sharpspring_form'); if (bodyNodeList.length === 0) { return; } var formNodeList = bodyNodeList[0].getElementsByTagName('form'); if (formNodeList.length === 0) { return; } var trackingInputNodeList = formNodeList[0].querySelectorAll('input[name="trackingid__sb"]'); var trackingInput; // find tracking input or create one if it doesn't exist if (trackingInputNodeList.length !== 0) { trackingInput = trackingInputNodeList[0]; } else { trackingInput = document.createElement('input'); trackingInput.type = 'hidden'; trackingInput.name = 'trackingid__sb'; formNodeList[0].appendChild(trackingInput); } // add tracking id to tracking input if it's not there if (trackingInput.value === '') { if (e && e.data && e.data.trackingID) { trackingInput.value = e.data.trackingID; } } $.getJSON(formDataURL, getParams, parseFormData); // remove event listener as this should only execute once

	removeEventer(messageEvent, onTrackingIDBackupMessageReceived); } eventer (messageEvent, onTrackingIDBackupMessageReceived); // Let the SS tracking script know we are ready to receive the tracking ID window.parent.postMessage({'trackingID': "?"}, '*'); } trackingIDBackup(); var free_email_providers; const url = "/includes/js/app /freeemailproviderlist.json"; fetch(url) .then(response => { return response.json(); }) .then (data => {free_email_providers = data;}) </script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	1
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informativo	**Re-examine Cache-control Directives**
Descrição	The cache-control header has not been set properly or is missing, allowing the browser and pro
URL	https://15560714.fls.doubleclick.net/activityi;src=15560714;type=visit0;cat=visit0;ord=91877040 tag_exp=101509157~103116026~103200004~103233427~104527906~104528501~10468420
Método	GET
Ataque	
Evidence	private, max-age=0
Other Info	
URL	https://app-3qnu8i2v1y.marketingautomation.services/prospector/getFormData/MzawMLE0NTM
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://carmelhoteis.com.br/
Método	GET
Ataque	
Evidence	
Other Info	
URL	https://www.google.com/pagead/1p-conversion/17102942276/? random=1758399955021&cv=11&fst=1758399955021&bg=ffffff&guid=ON&async=1&en=purch 3A%2F%2Fcarmelhoteis.com.br%2F&label=L4q8CNGg-8saEMTgqNs_&frm=0&tiba=Carmel%2
Método	GET
Ataque	
Evidence	no-cache, must-revalidate
Other Info	
Instances	4
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, mus
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control

	https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informativo	**Retrieved from Cache**
Descrição	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://static.doubleclick.net/instream/ad_status.js
Método	GET
Ataque	
Evidence	Age: 109
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://tag.goadopt.io/injector.js/v2/0017?website_code=04f3aae2-99c2-4f51-81ae-95070b7ea85f
Método	GET
Ataque	
Evidence	Age: 788629
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
URL	https://tag.goadopt.io/injector.js?website_code=04f3aae2-99c2-4f51-81ae-95070b7ea85f
Método	GET
Ataque	
Evidence	Age: 824023
Other Info	The presence of the 'Age' header indicates that a HTTP/1.1 compliant caching server is in use.
Instances	3
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	
WASC Id	
Plugin Id	10050

Informativo	Session Management Response Identified
Descrição	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	https://koi-3qnu8i2v1y.marketingautomation.services/koi?rf=&hn=carmelhoteis.com.br&lg=en-US&sr=1920x1080&cd=24&vr=2.4.1&se=1758399043254&tk=202509%7C68cf0a4304006702a43af8de&ac=KOI-4KR91Q9G7C&ts=1758399955&pt=NaN&pl=NaN&loc=https%3A%2F%2Fcarmelhoteis.com.br%2F&tp=page&ti=Carmel%20Hot%C3%A9is
Método	GET
Ataque	
Evidence	202509%7C68cf0a4304006702a43af8de
Other Info	cookie:koitk
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112