ZAP Scanning Report

Sites: https://booking.com http://booking.com

Generated on pon., 9 sty 2023 12:26:52

Summary of Alerts

Poziom ryzyka	Number of Alerts
Wysoki	0
redni	5
Niski	8
Informacyjny	5

Zagrozenia

Nazwa	Poziom ryzyka	Number of Instances
Absence of Anti-CSRF Tokens	redni	2
Content Security Policy (CSP) Header Not Set	redni	16
HTTP to HTTPS Insecure Transition in Form Post	redni	2
Hidden File Found	redni	4
Missing Anti-clickjacking Header	redni	1
Cookie No HttpOnly Flag	Niski	75
Cookie Without Secure Flag	Niski	74
Cookie with SameSite Attribute None	Niski	1
Cookie without SameSite Attribute	Niski	75
Cross-Domain JavaScript Source File Inclusion	Niski	41
Strict-Transport-Security Header Not Set	Niski	15
Timestamp Disclosure - Unix	Niski	1
X-Content-Type-Options Header Missing	Niski	2
Content Security Policy (CSP) Report-Only Header Found	Informacyjny	1
Information Disclosure - Suspicious Comments	Informacyjny	5
Modern Web Application	Informacyjny	1
Re-examine Cache-control Directives	Informacyjny	1
User Agent Fuzzer	Informacyjny	36

Alert Detail

redni	Absence of Anti-CSRF Tokens
	No Anti-CSRF tokens were found in a HTML submission form. Cross-site request forgery jest atakiem, który obejmuje zmuszanie ofiary do wysania dania HTTP do miejsca celowego bez ich wiedzy lub intencji w celu przeprowadzenia akcji jako ofiara. Podstawow przyczyn jest powtarzalno dziaania aplikacji z przewidywalnymi

Opis	adresami URL / formularzami. Charakterem ataku jest to, e CSRF wykorzystuje zaufanie, jakie witryna darzy uytkownika. Natomiast skrypty cross-site scripting (XSS) wykorzystuj zaufanie, jakim uytkownik darzy stron internetow. Podobnie jak w przypadku XSS, ataki CSRF niekoniecznie musz by przekierowane na drug stron, ale mog by. Cross-site request forgery jest równie znane jako CSRF, XSRF, atak za jednym klikniciem, jazda na sesjach, zdezorientowany delegat i surfowanie po morzu. Ataki CSRF s skuteczne w wielu sytuacjach, w tym: * Ofiara ma aktywn sesj w witrynie docelowej. * Ofiara jest uwierzytelniona za porednictwem protokou HTTP w witrynie docelowej. * Ofiara jest w tej samej sieci lokalnej co strona docelowa. CSRF zosta uyty przede wszystkim do wykonania akcji przeciwko witrynie docelowej z wykorzystaniem przywilejów ofiary, ale odkryto najnowsze techniki udostpniania informacji poprzez uzyskanie dostpu do odpowiedzi. Ryzyko udostpnienia informacji dramatycznie wzrasta kiedy strona celu jest podatna na XSS, poniewa XSS moe by uyty jako platforma dla CSRF, wczajc w to atak obsugiwany w granicach polityki tego samego pochodzenia.
URL	http://booking.com
Metody	GET
Atak	
Evidence	<form class="a0ac39e217" action="https://www.booking.com/searchresults.en-gb.html" method="GET">
URL	http://booking.com
Metody	GET
Atak	
Evidence	<form action="https:&#47;&#47;www.booking.com&#47;newslettersubscribe.html" method="post" name="newsletterform" id="emk-footer" class="footerForm emk-subscription-entry-point " data-component="emk/subscription-entry-point emk/subscription-entry-point-feedback-msg" data-emk-entry-point-label="footer" >
Instances	2
Solution	Faza: Architektura i Projektowanie Uywaj sprawdzonej biblioteki lub struktury, które nie pozwalaj na wystpienie tego osabienia lub wprowadzaj konstrukcje, które sprawiaj, e to osabienie jest atwiejsze do uniknicia. Na przykad, uywaj pakietów anty-CSRF takich jak OWASP CSRFGuard. Faza: Implementacja Upewnij si, e twoja aplikacja jest wolna od kwestii cross-site scripting, poniewa wikszo obron CSRF mog by ominite przez kontrolowany przez atakujcego skrypt. Fazy: Architektura i Projektowanie Wygeneruj unikalny numer dla kadego formularza, umie go w formularzu i zweryfikuj warto jednorazow po otrzymaniu formularza. Upewnij si, e liczba nie bdzie przewidywalna (CWE-330). Zwró uwag na to, e moe to by ominite uywajc XSS. Identyfikuj zwaszcza niebezpieczne dziaania. Kiedy uytkownik przeprowadza niebezpieczn operacj, wylij odrbne danie potwierdzenia by upewni si, e uytkownik jest przeznaczony do przeprowadzenia tego dziaania. Zwró uwag na to, e moe to by ominite uywajc XSS. Uywaj regulacji Zarzdzania Sesj ESAPI.

	Ta kontrola obejmuje komponent dla CSRF. Nie uywaj metody GET dla adnego dania, która uruchamia zmian stanu. Faza: Implementacja Sprawd nagówek HTTP Referer, aby sprawdzi, czy danie pochodzi z oczekiwanej strony. To mogoby przerwa prawowit funkcjonalno, poniewa uytkownicy lub proxy mogyby zosta wyczone wysyajc dla Referer prywatnych powodów.
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

redni	Content Security Policy (CSP) Header Not Set
Opis	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://booking.com
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-articles-https-index-articles.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-articles-index-articles-https.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-discover-https-index.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-dsf-https-index-destinationfinder.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-dsf-index-destinationfinder-https.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-https-index.xml

Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-incr-closed-index-hotel-reviews-https_2017-04-20.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-incr-closed-index-hotel-reviews-https_2017-04-21.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-index-https.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-reviews-https-index.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-reviews-index-city-review-https.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-reviews-index-country-review-https.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-reviews-index-hotel-review-https.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-reviews-index-region-review-https.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-reviews-index-single-review-https.xml
Metody	GET
Atak	
Evidence	
Instances	16

Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
Reference	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/
CWE Id	693
WASC Id	15
Plugin Id	10038

redni	HTTP to HTTPS Insecure Transition in Form Post
Opis	This check looks for insecure HTTP pages that host HTTPS forms. The issue is that an insecure HTTP page can easily be hijacked through MITM and the secure HTTPS form can be replaced or spoofed.
URL	http://booking.com
Metody	GET
Atak	
Evidence	https://www.booking.com/newslettersubscribe.html
URL	http://booking.com
Metody	GET
Atak	
Evidence	https://www.booking.com/searchresults.en-gb.html
Instances	2
Solution	Use HTTPS for landing pages that host secure forms.
Reference	
CWE Id	319
WASC Id	15
Plugin Id	10041

redni	Hidden File Found
Opis	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
URL	http://booking.com/._darcs
Metody	GET
Atak	
Evidence	HTTP/1.1 301 Moved Permanently
URL	http://booking.com/.bzr
Metody	GET
Atak	
Evidence	HTTP/1.1 301 Moved Permanently
URL	http://booking.com/.hg

Metody	GET
Atak	
Evidence	HTTP/1.1 301 Moved Permanently
URL	http://booking.com/BitKeeper
Metody	GET
Atak	
Evidence	HTTP/1.1 301 Moved Permanently
Instances	4
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
CWE Id	538
WASC Id	13
Plugin Id	40035

redni	**Missing Anti-clickjacking Header**
Opis	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	http://booking.com
Metody	GET
Atak	
Evidence	
Instances	1
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Niski	**Cookie No HttpOnly Flag**
Opis	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	http://booking.com
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/
Metody	GET

Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/$
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*.en-gb.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*.hi.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*.ru.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*.tr.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*city_bookings
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*lang=en-gb
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*lang=ru
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*lang=tr
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*nofollow=1
Metody	GET
Atak	

Evidence	set-cookie: _pxhd
URL	https://booking.com/_frdtcr
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/alt_avail
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/anysearch.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/bas/
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/best-price-guarantee/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/book-now-pay-later/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/book.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/c360_v1_track
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/confirmation.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/deals-special-offers/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd

URL	https://booking.com/episode_times
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/event
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/flexiproduct
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/fragment.*.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/fragment.*.json
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/fragment.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/fragment.json
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/free-cancellation/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/general.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/get-instant-confirmation/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/go

Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/go$
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/gta_impression
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/honing.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/hotel/us/the-airstream-van.*.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/hotel_attractions
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/hotel_rt_onview
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/hotelsonmap.*.json
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/join_js_tracking
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/js_errors
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/load_times
Metody	GET

Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/log_rt_blocks_order
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/markers_on_map
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/monthly_minrates
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/mybooking.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/no-booking-fees/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.de.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.en.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.es.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.fr.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.html
Metody	GET
Atak	

Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.it.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.ja.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.nl.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.pl.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.pt.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.zh.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/product_header.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/pxbook
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/pxgo
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/region_attractions
Metody	GET
Atak	
Evidence	set-cookie: _pxhd

URL	https://booking.com/reviewlist.*.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/reviewlist.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/robots.txt
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/s/
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/secure-booking/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/sitemap.xml
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/squeak
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/srcompset.*.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/srcompset.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/track
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/vpmlogdesktopscreensize

Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/we-speak-your-language/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
Instances	75
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

Niski	**Cookie Without Secure Flag**
Opis	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://booking.com/
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/$
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*.en-gb.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*.hi.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*.ru.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*.tr.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*city_bookings

Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*lang=en-gb
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*lang=ru
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*lang=tr
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*nofollow=1
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/_frdtcr
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/alt_avail
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/anysearch.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/bas/
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/best-price-guarantee/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/book-now-pay-later/index.
Metody	GET

Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/book.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/c360_v1_track
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/confirmation.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/deals-special-offers/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/episode_times
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/event
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/flexiproduct
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/fragment.*.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/fragment.*.json
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/fragment.html
Metody	GET
Atak	

Evidence	set-cookie: _pxhd
URL	https://booking.com/fragment.json
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/free-cancellation/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/general.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/get-instant-confirmation/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/go
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/go$
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/gta_impression
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/honing.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/hotel/us/the-airstream-van.*.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/hotel_attractions
Metody	GET
Atak	
Evidence	set-cookie: _pxhd

URL	https://booking.com/hotel_rt_onview
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/hotelsonmap.*.json
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/join_js_tracking
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/js_errors
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/load_times
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/log_rt_blocks_order
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/markers_on_map
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/monthly_minrates
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/mybooking.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/no-booking-fees/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.de.html

Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.en.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.es.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.fr.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.it.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.ja.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.nl.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.pl.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.pt.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.zh.html
Metody	GET

Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/product_header.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/pxbook
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/pxgo
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/region_attractions
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/reviewlist.*.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/reviewlist.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/robots.txt
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/s/
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/secure-booking/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/sitemap.xml
Metody	GET
Atak	

Evidence	set-cookie: _pxhd
URL	https://booking.com/squeak
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/srcompset.*.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/srcompset.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/track
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/vpmlogdesktopscreensize
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/we-speak-your-language/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
Instances	74
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	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
CWE Id	614
WASC Id	13
Plugin Id	10011

Niski	**Cookie with SameSite Attribute None**
Opis	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	http://booking.com
Metody	GET
Atak	

Evidence	set-cookie: bkng
Instances	1
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Niski	**Cookie without SameSite Attribute**
Opis	A cookie has been set without the SameSite attribute, 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	http://booking.com
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/$
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*.en-gb.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*.hi.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*.ru.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*.tr.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*city_bookings
Metody	GET

Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*lang=en-gb
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*lang=ru
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*lang=tr
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/*nofollow=1
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/_frdtcr
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/alt_avail
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/anysearch.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/bas/
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/best-price-guarantee/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/book-now-pay-later/index.
Metody	GET
Atak	

Evidence	set-cookie: _pxhd
URL	https://booking.com/book.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/c360_v1_track
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/confirmation.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/deals-special-offers/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/episode_times
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/event
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/flexiproduct
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/fragment.*.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/fragment.*.json
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/fragment.html
Metody	GET
Atak	

Evidence	set-cookie: _pxhd
URL	https://booking.com/fragment.json
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/free-cancellation/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/general.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/get-instant-confirmation/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/go
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/go$
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/gta_impression
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/honing.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/hotel/us/the-airstream-van.*.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/hotel_attractions
Metody	GET
Atak	
Evidence	set-cookie: _pxhd

URL	https://booking.com/hotel_rt_onview
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/hotelsonmap.*.json
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/join_js_tracking
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/js_errors
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/load_times
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/log_rt_blocks_order
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/markers_on_map
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/monthly_minrates
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/mybooking.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/no-booking-fees/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.de.html

Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.en.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.es.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.fr.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.it.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.ja.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.nl.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.pl.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.pt.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/photo.zh.html
Metody	GET

Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/product_header.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/pxbook
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/pxgo
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/region_attractions
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/reviewlist.*.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/reviewlist.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/robots.txt
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/s/
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/secure-booking/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/sitemap.xml
Metody	GET
Atak	

Evidence	set-cookie: _pxhd
URL	https://booking.com/squeak
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/srcompset.*.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/srcompset.html
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/track
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/vpmlogdesktopscreensize
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
URL	https://booking.com/we-speak-your-language/index.
Metody	GET
Atak	
Evidence	set-cookie: _pxhd
Instances	75
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Niski	**Cross-Domain JavaScript Source File Inclusion**
Opis	The page includes one or more script files from a third-party domain.
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script type="text/javascript" nonce="aFP1F47ySPg69E0" src="https://cdn.cookielaw.org/consent/3ea94870-d4b1-483a-b1d2-faf1d982bb31/OtAutoBlock.js"></script>
URL	http://booking.com
Metody	GET
Atak	

Evidence	<script src="https://cf.bstatic.com/libs/current-script-polyfill/1.0.0/current-script-polyfill.min.js" nonce="aFP1F47ySPg69E0"><\/script>')</script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script type="text/javascript" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/libs/privacy-consent/releases/2.1.35/customer/cookie-banner.min.js" data-domain-script="3ea94870-d4b1-483a-b1d2-faf1d982bb31"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script crossorigin="anonymous" src="https://cf.bstatic.com/libs/promise/7.0.4/promise-7.0.4.min.js" nonce="aFP1F47ySPg69E0"><\/script>')</script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-BHAwarenessBanner-BHAwarenessBanner" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/119.8f4ac63a.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="bookingcom-genius-credit-book-and-unlock-mfe-pages-GeniusVipCampaignsIndexBanner-GeniusVipCampaignsIndexBanner" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/186.cf9c058f.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-UniqueStaysProperties" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/224.827ec030.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-SimilarPropertiesCarousel" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/348.5beb4804.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-Empty" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/435.2c7dd6aa.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
	<script async="async" crossorigin="anonymous" data-chunk="src-components-

Evidence	CovidBanner" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/513.20177c67.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-DestinationPostcardsDesktop-DestinationPostcardsDesktop" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/514.195267cf.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-GeniusSignInBanner-GeniusSignInBanner" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/527.8554f923.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-BasNDisplayBannerIndexPrimary" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/541.ed3de1de.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-HeroBanner-HeroBannerDesktop" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/579.9599bfd0.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-SecondaryBanner-SecondaryBannerDesktop" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/664.7f380e79.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="bookingcom-web-shell-header-mfe-components-GlobalAlerts" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/665.eaca8a55.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-JapanNewYearCarousel" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/685.d70afe73.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
	<script async="async" crossorigin="anonymous" data-chunk="src-components-

Evidence	FullWidthBannerDesktop-FullWidthBannerDesktop" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/736.71cd5248.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-TripTypesDestinationsCarousel-TripTypesDestinationsCarousel" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/748.6b2d9cc7.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-HomesGuestsLoveCarousel" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/76.cad9115e.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="bookingcom-search-web-searchresults-components-SearchBoxDesktopHorizontal-SearchBoxDesktopHorizontal" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/778.e0b42985.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-NearbyAlternateDestinationsCarousel-NearbyAlternateDestinationsCarousel" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/797.0a7ab817.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-GeniusSignInSheet-GeniusSignInSheet" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/802.32296d17.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="bookingcom-web-shell-header-mfe-components-AccommodationHeader" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/93.fea042d8.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-PropertyTypesCarousel" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/970.51865114.chunk.js"></script>
URL	http://booking.com
Metody	GET

Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="src-components-DomesticDestinationsCarousel-DomesticDestinationsCarousel" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/979.b2f375d2.chunk.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="client" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/bui-react.700ceb62.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="client" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/client.a6ed7153.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script async="async" crossorigin="anonymous" data-chunk="client" nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/psb/capla/static/js/vendors.dbb66199.js"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script src="https://cf.bstatic.com/static/js/core-deps-inlinedet_cloudfront_sd/6da0bf621035bb8a2f9c756d6a89dda03b2f7864.js" crossorigin nonce="aFP1F47ySPg69E0"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script class="crossorigin-check-js" src="https://cf.bstatic.com/static/js/crossorigin_check_cloudfront_sd/2454015045ef79168d452ff4e7f30bdadff0aa81.js" async crossorigin nonce="aFP1F47ySPg69E0"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script src="https://cf.bstatic.com/static/js/error_catcher_bec_cloudfront_sd/0acd2ada6c74d5dec978a04ea837952bdf050cd2.js" crossorigin nonce="aFP1F47ySPg69E0" ></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script crossorigin type="text/javascript" src="https://cf.bstatic.com/static/js/genius_vip_cloudfront_sd/f980dbafa6b20d980f25ca835a161e7cece00d9d.js" nonce="aFP1F47ySPg69E0"></script>
URL	http://booking.com

Metody	GET
Atak	
Evidence	<script src="https://cf.bstatic.com/static/js/index_cloudfront_sd/b75751f1b49010e8153bc55617e422e3c6d1a338.js" crossorigin nonce="aFP1F47ySPg69E0"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script src="https://cf.bstatic.com/static/js/jquery_cloudfront_sd/e1e8c0e862309cb4caf3c0d5fbea48bfb8eaad42.js" class="jquery-script-tag" crossorigin nonce="aFP1F47ySPg69E0"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script src="https://cf.bstatic.com/static/js/landingpage_cloudfront_sd/5e36f8c5d1e7143819864a07b3d0ea4dba8022bb.js" crossorigin nonce="aFP1F47ySPg69E0"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script src="https://cf.bstatic.com/static/js/lazy_load_images_cloudfront_sd/77204d4da4aa41b08b1a4062c8e66e4629550994.js" async crossorigin nonce="aFP1F47ySPg69E0"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script src="https://cf.bstatic.com/static/js/main_cloudfront_sd/ea3d01a5614dae05358b7fe415207283134b2dd8.js" crossorigin nonce="aFP1F47ySPg69E0"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script nonce="aFP1F47ySPg69E0" src="https://cf.bstatic.com/static/js/raf_cloudfront_sd/b9e5b0bcf00cff69d910550bedf9b680172d2b89.js" crossorigin></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script src="https://cf.bstatic.com/static/js/searchbox_cloudfront_sd/80fd7ec836fefef363b534bd320c7c54388a2e56.js" crossorigin nonce="aFP1F47ySPg69E0"></script>
URL	http://booking.com
Metody	GET
Atak	
Evidence	<script crossorigin type="text/javascript" src="https://cf.bstatic.com/static/js/sp-on-maps_cloudfront_sd/d30eef4dc5202875d4c3301b8a0e8ff09f9a0e28.js" nonce="aFP1F47ySPg69E0"></script>
Instances	41

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

Niski	**Strict-Transport-Security Header Not Set**
Opis	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://booking.com/sitembk-articles-https-index-articles.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-articles-index-articles-https.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-discover-https-index.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-dsf-https-index-destinationfinder.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-dsf-index-destinationfinder-https.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-https-index.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-incr-closed-index-hotel-reviews-https_2017-04-20.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-incr-closed-index-hotel-reviews-https_2017-04-21.xml
Metody	GET
Atak	

Evidence	
URL	https://booking.com/sitembk-index-https.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-reviews-https-index.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-reviews-index-city-review-https.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-reviews-index-country-review-https.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-reviews-index-hotel-review-https.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-reviews-index-region-review-https.xml
Metody	GET
Atak	
Evidence	
URL	https://booking.com/sitembk-reviews-index-single-review-https.xml
Metody	GET
Atak	
Evidence	
Instances	15
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html 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
CWE Id	319
WASC Id	15
Plugin Id	10035

Niski	**Timestamp Disclosure - Unix**
Opis	A timestamp was disclosed by the application/web server - Unix

URL	http://booking.com
Metody	GET
Atak	
Evidence	1673263422
Instances	1
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Plugin Id	10096

Niski	**X-Content-Type-Options Header Missing**
Opis	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://booking.com/logo
Metody	GET
Atak	
Evidence	
URL	https://booking.com/robots.txt
Metody	GET
Atak	
Evidence	
Instances	2
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	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informacyjny	**Content Security Policy (CSP) Report-Only Header Found**
Opis	The response contained a Content-Security-Policy-Report-Only header, this may indicate a work-in-progress implementation, or an oversight in promoting pre-Prod to Prod, etc. Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

URL	http://booking.com
Metody	GET
Atak	
Evidence	
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.
Reference	https://www.w3.org/TR/CSP2/ https://w3c.github.io/webappsec-csp/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Informacyjny	Information Disclosure - Suspicious Comments
Opis	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	http://booking.com
Metody	GET
Atak	
Evidence	from
URL	http://booking.com
Metody	GET
Atak	
Evidence	query
URL	http://booking.com
Metody	GET
Atak	
Evidence	select
URL	http://booking.com
Metody	GET
Atak	
Evidence	user
URL	http://booking.com
Metody	GET
Atak	
Evidence	where
Instances	5
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200

WASC Id	13
Plugin Id	10027

Informacyjny	Modern Web Application
Opis	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	http://booking.com
Metody	GET
Atak	
Evidence	<a href="#" class=" ot-preference-center-footer"> Manage cookie settings </a>
Instances	1
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informacyjny	Re-examine Cache-control Directives
Opis	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://booking.com/robots.txt
Metody	GET
Atak	
Evidence	
Instances	1
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching 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

Informacyjny	User Agent Fuzzer
Opis	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	http://booking.com
Metody	GET
Atak	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://booking.com
Metody	GET

Atak	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://booking.com
Metody	GET
Atak	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://booking.com
Metody	GET
Atak	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://booking.com
Metody	GET
Atak	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://booking.com
Metody	GET
Atak	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://booking.com
Metody	GET
Atak	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://booking.com
Metody	GET
Atak	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://booking.com
Metody	GET
Atak	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://booking.com
Metody	GET
Atak	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://booking.com
Metody	GET
Atak	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://booking.com

Metody	GET
Atak	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://booking.com/robots.txt
Metody	GET
Atak	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://booking.com/robots.txt
Metody	GET
Atak	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://booking.com/robots.txt
Metody	GET
Atak	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://booking.com/robots.txt
Metody	GET
Atak	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://booking.com/robots.txt
Metody	GET
Atak	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://booking.com/robots.txt
Metody	GET
Atak	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://booking.com/robots.txt
Metody	GET
Atak	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
URL	http://booking.com/robots.txt
Metody	GET
Atak	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://booking.com/robots.txt
Metody	GET
Atak	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://booking.com/robots.txt

Metody	GET
Atak	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://booking.com/robots.txt
Metody	GET
Atak	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://booking.com/robots.txt
Metody	GET
Atak	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
URL	http://booking.com/sitemap.xml
Metody	GET
Atak	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
URL	http://booking.com/sitemap.xml
Metody	GET
Atak	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
URL	http://booking.com/sitemap.xml
Metody	GET
Atak	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
URL	http://booking.com/sitemap.xml
Metody	GET
Atak	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
URL	http://booking.com/sitemap.xml
Metody	GET
Atak	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
URL	http://booking.com/sitemap.xml
Metody	GET
Atak	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
URL	http://booking.com/sitemap.xml
Metody	GET
Atak	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	

URL	http://booking.com/sitemap.xml
Metody	GET
Atak	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
URL	http://booking.com/sitemap.xml
Metody	GET
Atak	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
URL	http://booking.com/sitemap.xml
Metody	GET
Atak	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
URL	http://booking.com/sitemap.xml
Metody	GET
Atak	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
URL	http://booking.com/sitemap.xml
Metody	GET
Atak	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Instances	36
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104