Key-drop Raport

Site: http://key-drop.com

Generated on wt., 21 lis 2023 15:46:51

ZAP Version: 2.14.0

Summary of Alerts

Poziom ryzyka	Number of Alerts
Wysoki	0
redni	3
Niski	6
Informacyjny	2

Zagrozenia

Nazwa	Poziom ryzyka	Number of Instances
Absence of Anti-CSRF Tokens	redni	1
Content Security Policy (CSP) Header Not Set	redni	2
Missing Anti-clickjacking Header	redni	1
Cookie No HttpOnly Flag	Niski	3
Cookie without SameSite Attribute	Niski	4
Cross-Domain JavaScript Source File Inclusion	Niski	2
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Niski	3
Server Leaks Version Information via "Server" HTTP Response Header Field	Niski	5
X-Content-Type-Options Header Missing	Niski	2
Modern Web Application	Informacyjny	1
Session Management Response Identified	Informacyjny	1

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 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.

Opis	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://key-drop.com
Metody	GET
Atak	
Evidence	<form action="" id="hrefFm" method="post" name="hrefFm">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: ""].
Instances	1
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 https://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://key-drop.com
Metody	GET
Atak	
Evidence	
Other Info	
URL	http://key-drop.com/sitemap.xml
Metody	GET
Atak	
Evidence	
Other Info	
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
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	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://key-drop.com
Metody	GET
Atak	
Evidence	
Other Info	
Instances	1
	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.

Solution	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://key-drop.com
Metody	GET
Atak	
Evidence	Set-Cookie: COOKIE_SUPPORT
Other Info	
URL	http://key-drop.com
Metody	GET
Atak	
Evidence	Set-Cookie: GUEST_LANGUAGE_ID
Other Info	
URL	http://key-drop.com
Metody	GET
Atak	
Evidence	Set-Cookie: JSESSIONID
Other Info	
Instances	3
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 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://key-drop.com
Metody	GET
Atak	
Evidence	Set-Cookie: BIP_CPD_PR_80

Other Info	
URL	http://key-drop.com
Metody	GET
Atak	
Evidence	Set-Cookie: COOKIE_SUPPORT
Other Info	
URL	http://key-drop.com
Metody	GET
Atak	
Evidence	Set-Cookie: GUEST_LANGUAGE_ID
Other Info	
URL	http://key-drop.com
Metody	GET
Atak	
Evidence	Set-Cookie: JSESSIONID
Other Info	
Instances	4
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://key-drop.com
Metody	GET
Atak	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=AW-785174776"></ /script>
Other Info	
URL	http://key-drop.com
Metody	GET
Atak	
Evidence	<script async src="https://www.googletagmanager.com/gtag/js?id=G-8L29Y1TGMQ"></ /script>
Other Info	
Instances	2
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	**Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**
Opis	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	http://key-drop.com
Metody	GET
Atak	
Evidence	X-Powered-By: PHP/5.3.3
Other Info	
URL	http://key-drop.com/
Metody	GET
Atak	
Evidence	X-Powered-By: PHP/5.3.3
Other Info	
URL	http://key-drop.com/sitemap.xml
Metody	GET
Atak	
Evidence	X-Powered-By: PHP/5.3.3
Other Info	
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10037

Niski	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Opis	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	http://key-drop.com
Metody	GET
Atak	
Evidence	1_1
Other	

Info	
URL	http://key-drop.com
Metody	GET
Atak	
Evidence	Apache/2.2.15 (Oracle)
Other Info	
URL	http://key-drop.com/
Metody	GET
Atak	
Evidence	Apache/2.2.15 (Oracle)
Other Info	
URL	http://key-drop.com/robots.txt
Metody	GET
Atak	
Evidence	Apache/2.2.15 (Oracle)
Other Info	
URL	http://key-drop.com/sitemap.xml
Metody	GET
Atak	
Evidence	Apache/2.2.15 (Oracle)
Other Info	
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10036

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	http://key-drop.com
Metody	GET
Atak	
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	http://key-drop.com/robots.txt
Metody	GET
Atak	
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	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	**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://key-drop.com
Metody	GET
Atak	
Evidence	
Other Info	Links have been found that do not have traditional href attributes, 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

Informacyjny	**Session Management Response Identified**
Opis	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	http://key-drop.com
Metody	GET
Atak	

Evidence	C0CD39057466230381C366F0C04DD01E
Other Info	cookie:JSESSIONID cookie:BIP_CPD_PR_80
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