ZAP Scanning Report

Sites: http://masiso.pl https://masiso.pl

Generated on wt., 27 lut 2024 13:09:09

ZAP Version: 2.14.0

Summary of Alerts

Poziom ryzyka	Number of Alerts
Wysoki	4
redni	5
Niski	10
Informacyjny	8

Zagrozenia

Nazwa	Poziom ryzyka	Number of Instances
Obchodzenie cieki	Wysoki	2
SQL Injection	Wysoki	1
SQL Injection - Oracle - Time Based	Wysoki	5
SQL Injection - SQLite	Wysoki	25
Absence of Anti-CSRF Tokens	redni	39
CSP: Wildcard Directive	redni	59
CSP: script-src unsafe-inline	redni	59
CSP: style-src unsafe-inline	redni	59
Missing Anti-clickjacking Header	redni	21
Big Redirect Detected (Potential Sensitive Information Leak)	Niski	48
Cookie No HttpOnly Flag	Niski	13
Cookie without SameSite Attribute	Niski	13
Cross-Domain JavaScript Source File Inclusion	Niski	35
Private IP Disclosure	Niski	1
Secure Pages Include Mixed Content	Niski	8
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Niski	71
Strict-Transport-Security Header Not Set	Niski	390
Timestamp Disclosure - Unix	Niski	45
X-Content-Type-Options Header Missing	Niski	366
Charset Mismatch	Informacyjny	6
Cookie Poisoning	Informacyjny	3
Information Disclosure - Suspicious Comments	Informacyjny	62
Modern Web Application	Informacyjny	17

Re-examine Cache-control Directives	Informacyjny	62
Retrieved from Cache	Informacyjny	2
Session Management Response Identified	Informacyjny	215
User Controllable HTML Element Attribute (Potential XSS)	Informacyjny	78

Alert Detail

Wysoki	Obchodzenie cieki
Opis	Technika ataku Obchodzenie cieki / Path Traversal umoliwia atakujcemu dostp do plików, katalogów i polece, które potencjalnie znajduj si poza gównym katalogiem dokumentów internetowych. Osoba atakujca moe manipulowa adresem URL w taki sposób, e strona internetowa bdzie wykonywa lub ujawnia zawarto dowolnych plików w dowolnym miejscu na serwerze sieciowym. Kade urzdzenie, które udostpnia interfejs oparty na HTTP, jest potencjalnie naraone na dziaanie ataku Path Traversal. Wikszo witryn internetowych ogranicza dostp uytkownika do okrelonej czci systemu plików, zwykle nazywanej katalogiem "katalog gówny dokumentu sieciowego" lub "katalog gówny CGI". Katalogi te zawieraj pliki przeznaczone do uzyskiwania dostpu przez uytkownika oraz plik wykonywalny niezbdny do sterowania funkcjami aplikacji internetowych. Aby uzyska dostp do plików lub wykonywa polecenia w dowolnym miejscu systemu plików, ataki Obchodzenia cieki bd wykorzystywa cechy sekwencji znaków specjalnych. Najbardziej podstawowy atak Obchodzenia cieki wykorzystuje sekwencj znaków specjalnych "../" w celu zmiany danej lokalizacji zasobu w adresie URL. Chocia najpopularniejsze serwery internetowe zapobiegn wyjciu z gównego katalogu dokumentów internetowych, alternatywne kodowanie sekwencji "../" moe pomóc omin filtry bezpieczestwa. Te odmiany metod zawieraj poprawne i niepoprawne kodowanie Unicode ("..%u2216" lub "..%c0%af") znaku ukonika, znaków ukonika odwrotnego ("..\") na serwerach Windows, zakodowanych w adresach URL znaki "%2e%2e%2f") i podwójne kodowanie URL ("..%255c") znaku ukonika odwrotnego. Nawet jeli serwer sieciowy waciwie ograniczy próby Obejcia cieki w ciece adresu URL, sama aplikacja internetowa moe nadal by podatna z powodu niewaciwej obsugi danych wprowadzanych przez uytkownika. Jest to powszechny problem aplikacji internetowych, które korzystaj z mechanizmów szablonów lub aduj tekst statyczny z plików. W odmianach tego ataku, oryginalna warto parametru adresu URL jest zastpowana nazw pliku jednego ze skryptów dynamicznych aplikacji WWW. W rezultacie wyniki mog ujawni kod ródowy, poniewa plik jest interpretowany jako tekst, a nie skrypt wykonywalny. These techniques often employ additional special characters such as the dot (".") to reveal the listing of the current working directory, or "%00" NULL characters in order to bypass rudimentary file extension checks.
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=%2Fembed
Metody	GET
Atak	/embed
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=%2Fembed
Metody	GET
Atak	/embed
Evidence	
Other Info	
Instances	2

Solution	Zakadaj, e wszystkie dane wejciowe s szkodliwe. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Odrzucaj wszystkie dane wejciowe, które nie s cile dopasowane ze specyfikacjami lub przeobra je w takie, które s dopasowane. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. Kiedy przeprowadzasz weryfikacj danych wejciowych, bierz pod uwag wszystkie potencjalnie wane waciwoci, wczajc dugo, peny zasig akceptowalnych wartoci, brakujcych lub dodatkowych danych wejciowych, zgodno poprzez wane pola i dostosowanie si do zasad sprawy. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." For filenames, use stringent allow lists that limit the character set to be used. Jeli to moliwe, zezwól tylko na pojedynczy "." znak w nazwie pliku, aby unikn saboci i wykluczy separatory katalogów, takie jak "/". Use an allow list of allowable file extensions. Uwaga jeli próbujesz oczyci dane, zrób tak, aby efekt kocowy nie by w formie, która moe by niebezpieczna. Mechanizm dezynfekcji moe usuwa znaki takie jak "." i ';' , które mog by wymagane w przypadku niektórych podatnoci. Osoba atakujca moe próbowa oszuka mechanizm czyszczcy w celu "oczyszczenia" danych do niebezpiecznej formy. Zaómy, e atakujcy wstrzykuje "." wewntrz nazwy pliku (np. "sensi.tiveFile") i mechanizm sanityzacji usuwa znak, który daje prawidow nazw pliku "sensitiveFile". Jeli dane wejciowe zostan teraz uznane za bezpieczne, plik moe zosta naruszony. Dane wejciowe powinny by dekodowane i kanonizowane do biecej wewntrznej reprezentacji przed weryfikacj. Upewnij si, e twoja aplikacja nie dekoduje tego samego wejcia dwukrotnie. Such errors could be used to bypass allow list schemes by introducing dangerous inputs after they have been checked. Uyj wbudowanej funkcji kanonizacji cieki (takiej jak realpath() w C), która produkuje kanoniczn wersj nazwy cieki, która skutecznie usuwa sekwencje ".." i dowizania symboliczne. Uruchom swój kod uywajc najmniejszych przywilejów, które s wymagane do wykonania koniecznych zada. Jeli moliwe, utwórz odizolowane konta z limitowanymi przywilejami, które s uywane tylko do pojedynczych zada. T drog, skuteczny atak nie da gwatownie dostpu do reszty oprogramowania lub jego rodowiska. Na przykad, baza danych aplikacji rzadko musi uruchomi baz danych administratora zwaszcza w codziennych operacjach. Kiedy zbiór akceptowalnych obiektów, takich jak nazwy plików lub adresy URL, jest ograniczony lub znany, utwórz odwzorowanie ze zbioru staych wartoci wejciowych (takich jak identyfikatory numeryczne) do rzeczywistych nazw plików lub adresów URL i odrzu wszystkie inne dane wejciowe. Uruchom swój kod w rodowisku "wizienia" lub podobnym rodowisku piaskownicy, które wymusza cise granice midzy procesem a systemem operacyjnym. Moe to skutecznie ograniczy, które pliki mog by dostpne w okrelonym katalogu lub które polecenia mog by wykonywane przez twoje oprogramowanie. Przykady poziomu OS obejmujce Unix chroot jail, AppArmor, and SELinux. Na zasadach ogólnych, zarzdzany kod moe zapewni pewn ochron. Na przykad,, java.io.FilePermission w Menaderze Ochrony Javy umoliwia ci sprecyzowa ograniczenia odnonie operacji na plikach. To moe nie by wykonalne rozwizanie i ogranicza wpyw tylko na system operacyjny; reszta aplikacji moe wci by podatna na zagroenie.
Reference	http://projects.webappsec.org/Path-Traversal https://cwe.mitre.org/data/definitions/22.html
CWE Id	22
WASC Id	33
Plugin Id	6

Wysoki	**SQL Injection**

Opis	SQL injection may be possible.
URL	https://masiso.pl/?p=26-2
Metody	GET
Atak	26-2
Evidence	
Other Info	The original page results were successfully replicated using the expression [26-2] as the parameter value The parameter value being modified was stripped from the HTML output for the purposes of the comparison
Instances	1
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40018

Wysoki	**SQL Injection - Oracle - Time Based**
Opis	SQL injection may be possible.
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	field: [action], value [lostpassword' / (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name ('10.0.0.5') from dual) / ']
Evidence	
Other	The query time is controllable using parameter value [lostpassword' / (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name ('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual

Info	union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual) / '], which caused the request to take [7 404] milliseconds, when the original unmodified query with value [lostpassword] took [410] milliseconds
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	field: [et_pb_contact_nazwa_rezerwacji_0], value [ZAP' / (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual) / ']
Evidence	
Other Info	The query time is controllable using parameter value [ZAP' / (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual) / '], which caused the request to take [8 169] milliseconds, when the original unmodified query with value [ZAP] took [2 048] milliseconds
URL	https://masiso.pl/menu/
Metody	POST
Atak	field: [_wpnonce-et-pb-contact-form-submitted-0], value [9e1ce563fe" / (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual) / '']
Evidence	
Other Info	The query time is controllable using parameter value [9e1ce563fe" / (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual) / ''], which caused the request to take [8 479] milliseconds, when the original unmodified query with value [9e1ce563fe] took [1 914] milliseconds
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	field: [et_pb_contactform_submit_0], value [(SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual)]
Evidence	
Other Info	The query time is controllable using parameter value [(SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual)], which caused the request to take [8 779] milliseconds, when the original unmodified query with value [et_contact_proccess] took [2 615] milliseconds
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	field: [redirect_to], value [" / (SELECT UTL_INADDR.get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual) / '']
Evidence	

Other Info	The query time is controllable using parameter value [" / (SELECT UTL_INADDR. get_host_name('10.0.0.1') from dual union SELECT UTL_INADDR.get_host_name ('10.0.0.2') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.3') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.4') from dual union SELECT UTL_INADDR.get_host_name('10.0.0.5') from dual) / "], which caused the request to take [7 405] milliseconds, when the original unmodified query with value [] took [386] milliseconds
Instances	5
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40021

Wysoki	**SQL Injection - SQLite**
Opis	SQL injection may be possible.
URL	https://masiso.pl/wp-content/et-cache/26/et-core-unified-tb-34-tb-53-deferred-26.min.css?ver=1707943770
Metody	GET
Atak	case randomblob(100000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [282] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [372] milliseconds, when the original unmodified query with value [1707943770] took [196] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [282] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [372] milliseconds, when the original unmodified query with value [1707943770] took [196] milliseconds.
URL	https://masiso.pl/wp-content/litespeed/ucss/59e4f0d94576502eef2f5818799f2db9.css?ver=d1918

Metody	GET
Atak	case randomblob(100000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [358] milliseconds, parameter value [case randomblob(1000000000) when not null then 1 else 1 end], which caused the request to take [1 396] milliseconds, when the original unmodified query with value [d1918] took [162] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [358] milliseconds, parameter value [case randomblob(1000000000) when not null then 1 else 1 end], which caused the request to take [1 396] milliseconds, when the original unmodified query with value [d1918] took [162] milliseconds.
URL	https://masiso.pl/wp-content/litespeed/ucss/8a08b99bd17c5d702188cdc5490812b0.css?ver=d1918
Metody	GET
Atak	case randomblob(100000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [1 298] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1 382] milliseconds, when the original unmodified query with value [d1918] took [220] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [1 298] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1 382] milliseconds, when the original unmodified query with value [d1918] took [220] milliseconds.
URL	https://masiso.pl/wp-content/litespeed/ucss/c9062085856c834a38b2cc78ed57756e.css?ver=d1918
Metody	GET
Atak	case randomblob(10000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 281] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1 362] milliseconds, when the original unmodified query with value [d1918] took [163] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 281] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1 362] milliseconds, when the original unmodified query with value [d1918] took [163] milliseconds.
URL	https://masiso.pl/wp-includes/js/underscore.min.js?ver=1.13.4
Metody	GET
Atak	case randomblob(100000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [1 342] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1 603] milliseconds, when the original unmodified query with value [1.13.4] took [178] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [1 342] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1 603] milliseconds, when the original unmodified query with value [1.13.4] took [178] milliseconds.
URL	https://masiso.pl/wp-includes/js/wp-util.min.js?ver=6.4.2
Metody	GET

Atak	case randomblob(100000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [248] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1 252] milliseconds, when the original unmodified query with value [6.4.2] took [149] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [248] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1 252] milliseconds, when the original unmodified query with value [6.4.2] took [149] milliseconds.
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	case randomblob(10000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [426] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1 375] milliseconds, when the original unmodified query with value [lostpassword] took [373] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [426] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1 375] milliseconds, when the original unmodified query with value [lostpassword] took [373] milliseconds.
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	case randomblob(10000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 391] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [3 436] milliseconds, when the original unmodified query with value [https://masiso.pl/wp-admin/] took [1 380] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 391] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [3 436] milliseconds, when the original unmodified query with value [https://masiso.pl/wp-admin/] took [1 380] milliseconds.
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	case randomblob(10000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 374] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [3 412] milliseconds, when the original unmodified query with value [en_GB] took [403] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 374] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [3 412] milliseconds, when the original unmodified query with value [en_GB] took [403] milliseconds.
URL	https://masiso.pl/
Metody	POST
Atak	case randomblob(1000000) when not null then 1 else 1 end
	The query time is controllable using parameter value [case randomblob(1000000) when not

Evidence	null then 1 else 1 end], which caused the request to take [1 909] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [2 197] milliseconds, when the original unmodified query with value [9e1ce563fe] took [2 337] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1 909] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [2 197] milliseconds, when the original unmodified query with value [9e1ce563fe] took [2 337] milliseconds.
URL	https://masiso.pl/
Metody	POST
Atak	case randomblob(10000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 345] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1 386] milliseconds, when the original unmodified query with value [ZAP] took [1 532] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 345] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1 386] milliseconds, when the original unmodified query with value [ZAP] took [1 532] milliseconds.
URL	https://masiso.pl/
Metody	POST
Atak	case randomblob(10000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 371] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1 473] milliseconds, when the original unmodified query with value [ZAP] took [1 215] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 371] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1 473] milliseconds, when the original unmodified query with value [ZAP] took [1 215] milliseconds.
URL	https://masiso.pl/
Metody	POST
Atak	case randomblob(10000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 876] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [2 027] milliseconds, when the original unmodified query with value [] took [1 442] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 876] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [2 027] milliseconds, when the original unmodified query with value [] took [1 442] milliseconds.
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	case randomblob(100000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [1 130] milliseconds, parameter

	value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [2 163] milliseconds, when the original unmodified query with value [] took [1 057] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [1 130] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [2 163] milliseconds, when the original unmodified query with value [] took [1 057] milliseconds.
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	case randomblob(100000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [1 684] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [2 509] milliseconds, when the original unmodified query with value [et_contact_proccess] took [1 049] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [1 684] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [2 509] milliseconds, when the original unmodified query with value [et_contact_proccess] took [1 049] milliseconds.
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	case randomblob(10000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 059] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1 283] milliseconds, when the original unmodified query with value [/kontakt/] took [1 014] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 059] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1 283] milliseconds, when the original unmodified query with value [/kontakt/] took [1 014] milliseconds.
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	case randomblob(1000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1 131] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [2 431] milliseconds, when the original unmodified query with value [9e1ce563fe] took [1 930] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1 131] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [2 431] milliseconds, when the original unmodified query with value [9e1ce563fe] took [1 930] milliseconds.
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	case randomblob(10000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 111] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [2 048] milliseconds, when the original unmodified query with value [ZAP] took [2 249] milliseconds.

Other Info	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 111] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [2 048] milliseconds, when the original unmodified query with value [ZAP] took [2 249] milliseconds.
URL	https://masiso.pl/menu/
Metody	POST
Atak	case randomblob(100000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1 505] milliseconds, parameter value [case randomblob(1000000000) when not null then 1 else 1 end], which caused the request to take [1 650] milliseconds, when the original unmodified query with value [/menu/] took [1 564] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [1 505] milliseconds, parameter value [case randomblob(1000000000) when not null then 1 else 1 end], which caused the request to take [1 650] milliseconds, when the original unmodified query with value [/menu/] took [1 564] milliseconds.
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	case randomblob(100000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [1 859] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [2 317] milliseconds, when the original unmodified query with value [9e1ce563fe] took [1 341] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [1 859] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [2 317] milliseconds, when the original unmodified query with value [9e1ce563fe] took [1 341] milliseconds.
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	case randomblob(10000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 695] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [4 732] milliseconds, when the original unmodified query with value [ZAP] took [1 476] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 695] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [4 732] milliseconds, when the original unmodified query with value [ZAP] took [1 476] milliseconds.
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	case randomblob(1000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [2 598] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [3 146] milliseconds, when the original unmodified query with value [] took [1 851] milliseconds.
Other	The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [2 598] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the

Info	request to take [3 146] milliseconds, when the original unmodified query with value [] took [1 851] milliseconds.
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	case randomblob(100000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [980] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1 197] milliseconds, when the original unmodified query with value [ZAP] took [960] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(100000) when not null then 1 else 1 end], which caused the request to take [980] milliseconds, parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [1 197] milliseconds, when the original unmodified query with value [ZAP] took [960] milliseconds.
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	case randomblob(10000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [441] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [442] milliseconds, when the original unmodified query with value [https://masiso.pl/wp-admin/] took [1 358] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [441] milliseconds, parameter value [case randomblob(100000000) when not null then 1 else 1 end], which caused the request to take [442] milliseconds, when the original unmodified query with value [https://masiso.pl/wp-admin/] took [1 358] milliseconds.
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	case randomblob(1000000) when not null then 1 else 1 end
Evidence	The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [586] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 413] milliseconds, when the original unmodified query with value [] took [488] milliseconds.
Other Info	The query time is controllable using parameter value [case randomblob(1000000) when not null then 1 else 1 end], which caused the request to take [586] milliseconds, parameter value [case randomblob(10000000) when not null then 1 else 1 end], which caused the request to take [1 413] milliseconds, when the original unmodified query with value [] took [488] milliseconds.
Instances	25
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality!

	Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40024

redni	**Absence of Anti-CSRF Tokens**
Opis	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. 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	https://masiso.pl
Metody	GET
Atak	
Evidence	<form class="et_pb_contact_form clearfix" method="post" action="https://masiso.pl/">
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: "_wp_http_referer" "_wpnonce-et-pb-contact-form-submitted-0" "et_pb_contact_email_0" "et_pb_contact_nazwa_rezerwacji_0" "et_pb_contactform_submit_0"].
URL	https://masiso.pl/
Metody	GET
Atak	
Evidence	<form class="et_pb_contact_form clearfix" method="post" action="https://masiso.pl/">

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: "_wp_http_referer" "_wpnonce-et-pb-contact-form-submitted-0" "et_pb_contact_email_0" "et_pb_contact_nazwa_rezerwacji_0" "et_pb_contactform_submit_0"].
URL	https://masiso.pl/?s
Metody	GET
Atak	
Evidence	<form role="search" method="get" action="https://masiso.pl/" class="wp-block-search__button-outside wp-block-search__text-button wp-block-search" >
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: "wp-block-search__input-1"].
URL	https://masiso.pl/author/damianpopiolgmail-com/
Metody	GET
Atak	
Evidence	<form role="search" method="get" action="https://masiso.pl/" class="wp-block-search__button-outside wp-block-search__text-button wp-block-search" >
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: "wp-block-search__input-1"].
URL	https://masiso.pl/gallery/740-2/
Metody	GET
Atak	
Evidence	<form role="search" method="get" action="https://masiso.pl/" class="wp-block-search__button-outside wp-block-search__text-button wp-block-search" >
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: "wp-block-search__input-1"].
URL	https://masiso.pl/gallery/740-2/
Metody	GET
Atak	
Evidence	<form class="et_pb_contact_form clearfix" method="post" action="https://masiso.pl/gallery/740-2/">
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 2: "_wp_http_referer" "_wpnonce-et-pb-contact-form-submitted-0" "et_pb_contact_email_0" "et_pb_contact_nazwa_rezerwacji_0" "et_pb_contactform_submit_0"].
URL	https://masiso.pl/gallery/740-2/feed/
Metody	GET
Atak	
Evidence	<form role="search" method="get" action="https://masiso.pl/" class="wp-block-search__button-outside wp-block-search__text-button wp-block-search" >
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: "wp-block-search__input-1"].
URL	https://masiso.pl/kontakt/
Metody	GET
Atak	
Evidence	<form class="et_pb_contact_form clearfix" method="post" action="https://masiso.pl/kontakt/" >
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: "_wp_http_referer" "_wpnonce-et-pb-contact-form-submitted-0" "et_pb_contact_email_0" "et_pb_contact_nazwa_rezerwacji_0" "et_pb_contactform_submit_0"].
URL	https://masiso.pl/menu/
Metody	GET
Atak	
Evidence	<form class="et_pb_contact_form clearfix" method="post" action="https://masiso.pl/menu/">
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: "_wp_http_referer" "_wpnonce-et-pb-contact-form-submitted-0" "et_pb_contact_email_0" "et_pb_contact_nazwa_rezerwacji_0" "et_pb_contactform_submit_0"].
URL	https://masiso.pl/o-restauracji/
Metody	GET
Atak	
Evidence	<form class="et_pb_contact_form clearfix" method="post" action="https://masiso.pl/o-restauracji/">
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: "_wp_http_referer" "_wpnonce-et-pb-contact-form-submitted-0" "et_pb_contact_email_0" "et_pb_contact_nazwa_rezerwacji_0" "et_pb_contactform_submit_0"].
URL	https://masiso.pl/page/2/?s
Metody	GET
Atak	
Evidence	<form role="search" method="get" action="https://masiso.pl/" class="wp-block-search__button-outside wp-block-search__text-button wp-block-search" >
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: "wp-block-search__input-1"].
URL	https://masiso.pl/polityka-prywatnosci/
Metody	GET
Atak	
Evidence	<form role="search" method="get" action="https://masiso.pl/" class="wp-block-search__button-outside wp-block-search__text-button wp-block-search" >
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: "wp-block-search__input-1"].
URL	https://masiso.pl/polityka-prywatnosci/

Metody	GET
Atak	
Evidence	<form class="et_pb_contact_form clearfix" method="post" action="https://masiso.pl/polityka-prywatnosci/">
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 2: "_wp_http_referer" "_wpnonce-et-pb-contact-form-submitted-0" "et_pb_contact_email_0" "et_pb_contact_nazwa_rezerwacji_0" "et_pb_contactform_submit_0"].
URL	https://masiso.pl/wp-login.php
Metody	GET
Atak	
Evidence	<form name="loginform" id="loginform" action="https://masiso.pl/wp-login.php" method="post">
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: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	https://masiso.pl/wp-login.php
Metody	GET
Atak	
Evidence	<form id="language-switcher" action="" method="get">
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 2: ""].
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	GET
Atak	
Evidence	<form name="lostpasswordform" id="lostpasswordform" action="https://masiso.pl/wp-login.php?action=lostpassword" method="post">
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: "redirect_to" "user_login" "wp-submit"].
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	GET
Atak	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "action"].
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	<form name="lostpasswordform" id="lostpasswordform" action="https://masiso.pl/wp-login.php?action=lostpassword" method="post">

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: "redirect_to" "user_login" "wp-submit"].
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "action"].
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	<form name="loginform" id="loginform" action="https://masiso.pl/wp-login.php" method="post">
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: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	<form name="loginform" id="loginform" action="https://masiso.pl/wp-login.php" method="post">
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: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].

URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	<form name="loginform" id="loginform" action="https://masiso.pl/wp-login.php" method="post">
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: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "redirect_to"].
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	<form name="loginform" id="loginform" action="https://masiso.pl/wp-login.php" method="post">
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: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	<form id="language-switcher" action="" method="get">
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 2: ""].
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	<form class="et_pb_contact_form clearfix" method="post" action="https://masiso.pl/">
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: "_wp_http_referer" "_wpnonce-et-pb-contact-form-submitted-0" "et_pb_contact_email_0" "et_pb_contact_nazwa_rezerwacji_0" "et_pb_contactform_submit_0"].
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	

Evidence	<form role="search" method="get" action="https://masiso.pl/" class="wp-block-search__button-outside wp-block-search__text-button wp-block-search" >
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: "wp-block-search__input-1"].
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	<form class="et_pb_contact_form clearfix" method="post" action="https://masiso.pl/gallery/740-2/">
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 2: "_wp_http_referer" "_wpnonce-et-pb-contact-form-submitted-0" "et_pb_contact_email_0" "et_pb_contact_nazwa_rezerwacji_0" "et_pb_contactform_submit_0"].
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	<form class="et_pb_contact_form clearfix" method="post" action="https://masiso.pl/kontakt/" >
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: "_wp_http_referer" "_wpnonce-et-pb-contact-form-submitted-0" "et_pb_contact_email_0" "et_pb_contact_nazwa_rezerwacji_0" "et_pb_contactform_submit_0"].
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	<form class="et_pb_contact_form clearfix" method="post" action="https://masiso.pl/menu/">
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: "_wp_http_referer" "_wpnonce-et-pb-contact-form-submitted-0" "et_pb_contact_email_0" "et_pb_contact_nazwa_rezerwacji_0" "et_pb_contactform_submit_0"].
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	<form class="et_pb_contact_form clearfix" method="post" action="https://masiso.pl/o-restauracji/">
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: "_wp_http_referer" "_wpnonce-et-pb-contact-form-submitted-0" "et_pb_contact_email_0" "et_pb_contact_nazwa_rezerwacji_0" "et_pb_contactform_submit_0"].
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	

Evidence	<form role="search" method="get" action="https://masiso.pl/" class="wp-block-search__button-outside wp-block-search__text-button wp-block-search" >
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: "wp-block-search__input-1"].
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	<form class="et_pb_contact_form clearfix" method="post" action="https://masiso.pl/polityka-prywatnosci/">
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 2: "_wp_http_referer" "_wpnonce-et-pb-contact-form-submitted-0" "et_pb_contact_email_0" "et_pb_contact_nazwa_rezerwacji_0" "et_pb_contactform_submit_0"].
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	<form name="loginform" id="loginform" action="https://masiso.pl/wp-login.php" method="post">
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: "redirect_to" "rememberme" "testcookie" "user_login" "user_pass" "wp-submit"].
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	<form id="language-switcher" action="" method="get">
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 2: ""].
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	<form name="lostpasswordform" id="lostpasswordform" action="https://masiso.pl/wp-login.php?action=lostpassword" method="post">
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: "redirect_to" "user_login" "wp-submit"].
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	<form id="language-switcher" action="" method="get">
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 2: "action"].

Instances	39
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	**CSP: Wildcard Directive**
Opis	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-

Info	ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/05/chilli.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/05/cos.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/05/dragon-stroke.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/05/fale-pattern-grey.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/05/fale-pattern-orange.svg
Metody	GET

Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/05/garlic.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/05/majeranek.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/05/ornament-pattern-gey2.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/05/ornament-pattern-orange2.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive

Info	(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/05/roslina.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/06/stars.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/08/Clock.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/08/Direction.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/09/contact-ko.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/09/menu-ko.svg
Metody	GET
Atak	

Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/09/pyszne-ko.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	http://masiso.pl/wp-content/uploads/2023/10/masiso-fav-icon.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/?p=24
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL	https://masiso.pl/?p=26
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/?p=28
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/?p=740
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/?p=855
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/?s
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/author/damianpopiolgmail-com/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/embed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/gallery/740-2/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/gallery/740-2/feed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/kontakt/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/kontakt/embed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/menu/

Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/menu/embed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/o-restauracji/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/o-restauracji/embed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/page/2/?s
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/polityka-prywatnosci/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-

Other Info	ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/polityka-prywatnosci/embed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/sitemap.html
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/wp-admin/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/wp-admin/admin-ajax.php
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/wp-login.php
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	GET

Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
	The following directives either allow wildcard sources (or ancestors), are not defined, or are

Other Info	overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/polityka-prywatnosci/

Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive (s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
Instances	59
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

redni	**CSP: script-src unsafe-inline**
Opis	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests

Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/chilli.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/cos.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/dragon-stroke.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/fale-pattern-grey.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/fale-pattern-orange.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/garlic.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.

URL	http://masiso.pl/wp-content/uploads/2023/05/majeranek.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/ornament-pattern-gey2.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/ornament-pattern-orange2.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/roslina.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/06/stars.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/08/Clock.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/08/Direction.svg
Metody	GET

Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/09/contact-ko.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/09/menu-ko.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/09/pyszne-ko.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/10/masiso-fav-icon.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/?p=24
Metody	GET
Atak	

Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/?p=26
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/?p=28
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/?p=740
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/?p=855
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/?s
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/author/damianpopiolgmail-com/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/embed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other	

Info	script-src includes unsafe-inline.
URL	https://masiso.pl/gallery/740-2/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/gallery/740-2/feed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/kontakt/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/kontakt/embed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/menu/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/menu/embed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/o-restauracji/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/o-restauracji/embed/

Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/page/2/?s
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/polityka-prywatnosci/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/polityka-prywatnosci/embed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/sitemap.html
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/wp-admin/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/wp-admin/admin-ajax.php
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php
Metody	GET

Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/
Metody	POST

Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	script-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	upgrade-insecure-requests

Other Info	script-src includes unsafe-inline.
Instances	59
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

redni	**CSP: style-src unsafe-inline**
Opis	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/chilli.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/cos.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/dragon-stroke.svg

Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/fale-pattern-grey.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/fale-pattern-orange.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/garlic.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/majeranek.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/ornament-pattern-gey2.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/ornament-pattern-orange2.svg
Metody	GET
Atak	

Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/05/roslina.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/06/stars.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/08/Clock.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/08/Direction.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/09/contact-ko.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/09/menu-ko.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/09/pyszne-ko.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests

Other Info	style-src includes unsafe-inline.
URL	http://masiso.pl/wp-content/uploads/2023/10/masiso-fav-icon.svg
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/?p=24
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/?p=26
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/?p=28
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/?p=740
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.

URL	https://masiso.pl/?p=855
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/?s
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/author/damianpopiolgmail-com/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/embed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/gallery/740-2/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/gallery/740-2/feed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/kontakt/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/kontakt/embed/
Metody	GET

Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/menu/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/menu/embed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/o-restauracji/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/o-restauracji/embed/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/page/2/?s
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/polityka-prywatnosci/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/polityka-prywatnosci/embed/
Metody	GET
Atak	

Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/sitemap.html
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/wp-admin/
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/wp-admin/admin-ajax.php
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	upgrade-insecure-requests

Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other	

Info	style-src includes unsafe-inline.
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	upgrade-insecure-requests
Other Info	style-src includes unsafe-inline.
Instances	59
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

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	https://masiso.pl
Metody	GET
Atak	
Evidence	
Other	

Info	
URL	https://masiso.pl/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/?s
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/author/damianpopiolgmail-com/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/gallery/740-2/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/kontakt/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/kontakt/embed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/menu/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/menu/embed/

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/o-restauracji/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/o-restauracji/embed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/page/2/?s
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/embed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/sitemap.html
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/
Metody	POST

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	
Other Info	
Instances	21
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	Big Redirect Detected (Potential Sensitive Information Leak)
Opis	The server has responded with a redirect that seems to provide a large response. This may indicate that although the server sent a redirect it also responded with body content (which may include sensitive details, PII, etc.).
URL	http://masiso.pl/wp-content/uploads/2023/05/bimbab.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 55 [https://masiso.pl/wp-content/uploads/2023/05/bimbab.jpg]. Predicted response size: 355. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/chicken-soup.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 61 [https://masiso.pl/wp-content/uploads/2023/05/chicken-soup.jpg]. Predicted response size: 361. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/chilli-chicken.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 63 [https://masiso.pl/wp-content/uploads/2023/05/chilli-chicken.jpg]. Predicted response size: 363. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 62 [https://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg]. Predicted response size: 362. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/chilli.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 55 [https://masiso.pl/wp-content/uploads/2023/05/chilli.svg]. Predicted response size: 355. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/cos.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 52 [https://masiso.pl/wp-content/uploads/2023/05/cos.svg]. Predicted response size: 352. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg
Metody	GET
Atak	
Evidence	

Other Info	Location header URI length: 60 [https://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg]. Predicted response size: 360. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/dragon-stroke.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 62 [https://masiso.pl/wp-content/uploads/2023/05/dragon-stroke.svg]. Predicted response size: 362. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/fale-pattern-grey.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 66 [https://masiso.pl/wp-content/uploads/2023/05/fale-pattern-grey.svg]. Predicted response size: 366. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/fale-pattern-orange.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 68 [https://masiso.pl/wp-content/uploads/2023/05/fale-pattern-orange.svg]. Predicted response size: 368. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/garlic.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 55 [https://masiso.pl/wp-content/uploads/2023/05/garlic.svg]. Predicted response size: 355. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/majeranek.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 58 [https://masiso.pl/wp-content/uploads/2023/05/majeranek.svg]. Predicted response size: 358. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 66 [https://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg]. Predicted response size: 366. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/ornament-pattern-gey2.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 70 [https://masiso.pl/wp-content/uploads/2023/05/ornament-pattern-gey2.svg]. Predicted response size: 370. Response Body Length: 795.

URL	http://masiso.pl/wp-content/uploads/2023/05/ornament-pattern-orange2.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 73 [https://masiso.pl/wp-content/uploads/2023/05/ornament-pattern-orange2.svg]. Predicted response size: 373. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/pattern-shape.png
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 62 [https://masiso.pl/wp-content/uploads/2023/05/pattern-shape.png]. Predicted response size: 362. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/05/roslina.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 56 [https://masiso.pl/wp-content/uploads/2023/05/roslina.svg]. Predicted response size: 356. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/06/Kimchicabbage.Perfectasanadditiontodishesoreatenseparately_.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 108 [https://masiso.pl/wp-content/uploads/2023/06/Kimchicabbage.Perfectasanadditiontodishesoreatenseparately_.jpg]. Predicted response size: 408. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/06/stars.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 54 [https://masiso.pl/wp-content/uploads/2023/06/stars.svg]. Predicted response size: 354. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Clock.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 54 [https://masiso.pl/wp-content/uploads/2023/08/Clock.svg]. Predicted response size: 354. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 62 [https://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi.jpg]. Predicted response size: 362. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Direction.svg

Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 58 [https://masiso.pl/wp-content/uploads/2023/08/Direction.svg]. Predicted response size: 358. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-1-682x1024.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 66 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-1-682x1024.jpg]. Predicted response size: 366. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-1.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 57 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-1.jpg]. Predicted response size: 357. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-31.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 58 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-31.jpg]. Predicted response size: 358. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-34-682x1024.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 67 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-34-682x1024.jpg]. Predicted response size: 367. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-6.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 57 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-6.jpg]. Predicted response size: 357. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-1024x683.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 75 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-1024x683.jpg]. Predicted response size: 375. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10.jpg
Metody	GET

Atak	
Evidence	
Other Info	Location header URI length: 67 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10.jpg]. Predicted response size: 367. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-14.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 67 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-14.jpg]. Predicted response size: 367. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-15.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 67 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-15.jpg]. Predicted response size: 367. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 67 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16.jpg]. Predicted response size: 367. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 67 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17.jpg]. Predicted response size: 367. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 67 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18.jpg]. Predicted response size: 367. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 67 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19.jpg]. Predicted response size: 367. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2.jpg
Metody	GET
Atak	
Evidence	

Other Info	Location header URI length: 66 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2.jpg]. Predicted response size: 366. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 67 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20.jpg]. Predicted response size: 367. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-1024x574.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 76 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-1024x574.jpg]. Predicted response size: 376. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 67 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21.jpg]. Predicted response size: 367. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 66 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5.jpg]. Predicted response size: 366. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 66 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6.jpg]. Predicted response size: 366. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 66 [https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9.jpg]. Predicted response size: 366. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/09/contact-ko.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 59 [https://masiso.pl/wp-content/uploads/2023/09/contact-ko.svg]. Predicted response size: 359. Response Body Length: 795.

URL	http://masiso.pl/wp-content/uploads/2023/09/menu-ko.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 56 [https://masiso.pl/wp-content/uploads/2023/09/menu-ko.svg]. Predicted response size: 356. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/09/pyszne-ko.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 58 [https://masiso.pl/wp-content/uploads/2023/09/pyszne-ko.svg]. Predicted response size: 358. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2023/10/masiso-fav-icon.svg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 64 [https://masiso.pl/wp-content/uploads/2023/10/masiso-fav-icon.svg]. Predicted response size: 364. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2024/01/Chefstirfryinwok.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 65 [https://masiso.pl/wp-content/uploads/2024/01/Chefstirfryinwok.jpg]. Predicted response size: 365. Response Body Length: 795.
URL	http://masiso.pl/wp-content/uploads/2024/01/TraditionalKoreanchickensoupwithhomemadenoodles-300x169.jpg
Metody	GET
Atak	
Evidence	
Other Info	Location header URI length: 104 [https://masiso.pl/wp-content/uploads/2024/01/TraditionalKoreanchickensoupwithhomemadenoodles-300x169.jpg]. Predicted response size: 404. Response Body Length: 795.
Instances	48
Solution	Ensure that no sensitive information is leaked via redirect responses. Redirect responses should have almost no content.
Reference	
CWE Id	201
WASC Id	13
Plugin Id	10044

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	https://masiso.pl/wp-login.php

Metody	GET
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	GET
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	set-cookie: wp_lang
Other Info	
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB

Metody	GET
Atak	
Evidence	set-cookie: wp_lang
Other Info	
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	set-cookie: wp_lang
Other Info	
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	set-cookie: tk_ai
Other Info	
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
Instances	13
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	https://masiso.pl/wp-login.php
Metody	GET
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	GET
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	set-cookie: wp_lang
Other Info	
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	

Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	set-cookie: wp_lang
Other Info	
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	set-cookie: wp_lang
Other Info	
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	set-cookie: tk_ai
Other Info	
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	set-cookie: wordpress_test_cookie
Other Info	
Instances	13
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	https://masiso.pl
Metody	GET
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	
URL	https://masiso.pl/
Metody	GET
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	
URL	https://masiso.pl/?s
Metody	GET
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	
URL	https://masiso.pl/author/damianpopiolgmail-com/
Metody	GET
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	
URL	https://masiso.pl/gallery/740-2/
Metody	GET
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	
URL	https://masiso.pl/gallery/740-2/feed/
Metody	GET
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	

URL	https://masiso.pl/kontakt/
Metody	GET
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	
URL	https://masiso.pl/menu/
Metody	GET
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	
URL	https://masiso.pl/o-restauracji/
Metody	GET
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	
URL	https://masiso.pl/page/2/?s
Metody	GET
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/
Metody	GET
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/slick-carousel/1.6.0/slick.js"></script>
Other Info	
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>

Other Info	
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=6Ld7n2MoAAAAAIebOIHHmyuGYoNMEb82esv38TIO&ver=4.23.4" id="et-recaptcha-v3-js"></script>
Other Info	
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://www.googletagmanager.com/gtag/js?id=G-79X3RFDRFF" id="google_gtagjs-js" async></script>
Other Info	
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/slick-carousel/1.6.0/slick.js"></script>
Other Info	
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=6Ld7n2MoAAAAAIebOIHHmyuGYoNMEb82esv38TIO&ver=4.23.4" id="et-recaptcha-v3-js"></script>
Other Info	
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://www.googletagmanager.com/gtag/js?id=G-79X3RFDRFF" id="google_gtagjs-js" async></script>
Other Info	
URL	https://masiso.pl/kontakt/
Metody	POST

Atak	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/slick-carousel/1.6.0/slick.js"></script>
Other Info	
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=6Ld7n2MoAAAAAIebOIHHmyuGYoNMEb82esv38TIO&ver=4.23.4" id="et-recaptcha-v3-js"></script>
Other Info	
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://www.googletagmanager.com/gtag/js?id=G-79X3RFDRFF" id="google_gtagjs-js" async></script>
Other Info	
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/slick-carousel/1.6.0/slick.js"></script>
Other Info	
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=6Ld7n2MoAAAAAIebOIHHmyuGYoNMEb82esv38TIO&ver=4.23.4" id="et-recaptcha-v3-js"></script>
Other Info	

URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://www.googletagmanager.com/gtag/js?id=G-79X3RFDRFF" id="google_gtagjs-js" async></script>
Other Info	
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/slick-carousel/1.6.0/slick.js"></script>
Other Info	
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>
Other Info	
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=6Ld7n2MoAAAAAIebOIHHmyuGYoNMEb82esv38TIO&ver=4.23.4" id="et-recaptcha-v3-js"></script>
Other Info	
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://www.googletagmanager.com/gtag/js?id=G-79X3RFDRFF" id="google_gtagjs-js" async></script>
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/slick-carousel/1.6.0/slick.js"></script>
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://stats.wp.com/e-202409.js" id="jetpack-stats-js" data-wp-strategy="defer"></script>

Other Info	
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=6Ld7n2MoAAAAAIebOIHHmyuGYoNMEb82esv38TIO&ver=4.23.4" id="et-recaptcha-v3-js"></script>
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	<script type="text/javascript" src="https://www.googletagmanager.com/gtag/js?id=G-79X3RFDRFF" id="google_gtagjs-js" async></script>
Other Info	
Instances	35
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	**Private IP Disclosure**
Opis	A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.
URL	https://masiso.pl/wp-content/uploads/2023/05/majeranek.svg
Metody	GET
Atak	
Evidence	10.94.83.53
Other Info	10.94.83.53
Instances	1
Solution	Remove the private IP address from the HTTP response body. For comments, use JSP/ASP/PHP comment instead of HTML/JavaScript comment which can be seen by client browsers.
Reference	https://tools.ietf.org/html/rfc1918
CWE Id	200
WASC Id	13
Plugin Id	2

Niski	**Secure Pages Include Mixed Content**
Opis	The page includes mixed content, that is content accessed via HTTP instead of HTTPS.
URL	https://masiso.pl/?s
Metody	GET
Atak	

Evidence	http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg
Other Info	tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg
URL	https://masiso.pl/page/2/?s
Metody	GET
Atak	
Evidence	http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg
Other Info	tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg
Other Info	tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/dragon-stroke.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Clock.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Direction.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/bimbab.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/chilli-chicken.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/09/pyszne-ko.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/Kimchicabbage.Perfectasanadditiontodishesoreatenseparately_.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/pattern-shape.png tag=img src=http://masiso.pl/wp-content/uploads/2023/05/bimbab.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/chicken-soup.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/roslina.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/cos.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/majeranek.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/roslina.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2024/01/Chefstirfryinwok.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg
Other Info	tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg
URL	https://masiso.pl/kontakt/

Metody	POST
Atak	
Evidence	http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg
Other Info	tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/dragon-stroke.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Clock.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Direction.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-1024x574.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-6.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/09/contact-ko.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/fale-pattern-orange.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-1.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-31.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg
Other Info	tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/dragon-stroke.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/chilli.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/09/menu-ko.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/cos.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-1024x683.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/garlic.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/roslina.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/chilli.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/cos.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-14.jpg tag=img src=http://masiso.pl/wp-content/uploads/2024/01/TraditionalKoreanchickensoupwithhomemadenoodles-300x169.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/majeranek.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/majeranek.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/chilli.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/roslina.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/cos.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	

Evidence	http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg
Other Info	tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/dragon-stroke.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Clock.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Direction.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-34-682x1024.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-1-682x1024.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/09/pyszne-ko.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/pattern-shape.png tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-6.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-15.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/majeranek.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/cos.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/majeranek.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-1.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/roslina.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2024/01/Chefstirfryinwok.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/06/stars.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20.jpg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg
Other Info	tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg tag=img src=http://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg
Instances	8
Solution	A page that is available over SSL/TLS must be comprised completely of content which is transmitted over SSL/TLS. The page must not contain any content that is transmitted over unencrypted HTTP. This includes content from third party sites.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
CWE Id	311
WASC Id	4
Plugin Id	10040

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	https://masiso.pl
Metody	GET
Atak	

Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/?p=24
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/?p=26
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/?p=28
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/?p=740
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/?p=855
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/?s
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27

Other Info	
URL	https://masiso.pl/author/damianpopiolgmail-com/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/author/damianpopiolgmail-com/feed/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/comments/feed/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/embed/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/feed/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/gallery/740-2/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/gallery/740-2/feed/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	

URL	https://masiso.pl/kontakt/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/kontakt/embed/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/menu/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/menu/embed/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/o-restauracji/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/o-restauracji/embed/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/page-sitemap.html
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/page-sitemap.xml
Metody	GET

Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/page/2/?s
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/embed/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/robots.txt
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/search/feed/rss2/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/sitemap-misc.html
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/sitemap-misc.xml
Metody	GET
Atak	

Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/sitemap.html
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/sitemap.xml
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-admin/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-admin/admin-ajax.php
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2F
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27

Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fkontakt%2F
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fmenu%2F
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fo-restauracji%2F
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fpolityka-prywatnosci%2F
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2F
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fkontakt%2F
Metody	GET

Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fmenu%2F
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fo-restauracji%2F
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fpolityka-prywatnosci%2F
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/pages/21
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/pages/24
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/pages/26
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/pages/28
Metody	GET

Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/pages/855
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/robogallery/740
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/users/1
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-login.php
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	

Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/xmlrpc.php
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/xmlrpc.php?rsd
Metody	GET
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	x-powered-by: PHP/8.1.27

Other Info	
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	x-powered-by: PHP/8.1.27
Other Info	
Instances	71
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	**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://masiso.pl
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/?s
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/author/damianpopiolgmail-com/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/author/damianpopiolgmail-com/feed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/comments/feed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/feed/

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/gallery/740-2/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/gallery/740-2/feed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/kontakt/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/kontakt/embed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/menu/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/menu/embed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/o-restauracji/
Metody	GET
Atak	

Evidence	
Other Info	
URL	https://masiso.pl/o-restauracji/embed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/page-sitemap.html
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/page-sitemap.xml
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/page/2/?s
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/embed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/robots.txt
Metody	GET
Atak	
Evidence	

Other Info	
URL	https://masiso.pl/search/feed/rss2/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/sitemap-misc.html
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/sitemap-misc.xml
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/sitemap.html
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/sitemap.xml
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-admin/admin-ajax.php
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-admin/css/forms.min.css?ver=6.4.2
Metody	GET
Atak	
Evidence	
Other Info	

URL	https://masiso.pl/wp-admin/css/l10n.min.css?ver=6.4.2
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-admin/css/login.min.css?ver=6.4.2
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-admin/js/password-strength-meter.min.js?ver=6.4.2
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-admin/js/user-profile.min.js?ver=6.4.2
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/21/et-core-unified-21.min.css?ver=1707943102
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/21/et-core-unified-tb-34-tb-53-deferred-21.min.css?ver=1707943104
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/21/et-divi-dynamic-tb-34-tb-53-21-late.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/21/et-divi-dynamic-tb-34-tb-53-21.css

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/24/et-core-unified-24.min.css?ver=1707943604
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/24/et-core-unified-tb-34-tb-53-deferred-24.min.css?ver=1707943605
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/24/et-divi-dynamic-tb-34-tb-53-24-late.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/24/et-divi-dynamic-tb-34-tb-53-24.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/26/et-core-unified-26.min.css?ver=1707943770
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/26/et-core-unified-tb-34-tb-53-deferred-26.min.css?ver=1707943770
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/26/et-divi-dynamic-tb-34-tb-53-26-late.css
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/26/et-divi-dynamic-tb-34-tb-53-26.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/28/et-core-unified-28.min.css?ver=1707943745
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/28/et-core-unified-tb-34-tb-53-deferred-28.min.css?ver=1707943745
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/28/et-divi-dynamic-tb-34-tb-53-28-late.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/28/et-divi-dynamic-tb-34-tb-53-28.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/53/et-core-unified-cpt-deferred-53.min.css?ver=1707943103
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/740/et-divi-dynamic-tb-34-tb-53-740.css
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/855/et-core-unified-tb-34-tb-53-deferred-855.min.css?ver=1708685896
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/855/et-divi-dynamic-tb-34-tb-53-855-late.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/855/et-divi-dynamic-tb-34-tb-53-855.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/global/et-divi-customizer-global.min.css?ver=1707943102
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/search/et-divi-dynamic-tb-34-tb-53-late.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/et-cache/search/et-divi-dynamic-tb-34-tb-53.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/litespeed/css/e4115894001a031ae7109874cbde969d.css?ver=d1918
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/litespeed/css/e7c5e2684e7d3e9da278582d302fa5e5.css?ver=d1918
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/litespeed/ucss/192a8138017bf2a127a035a2f9e72d20.css?ver=d1918
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/litespeed/ucss/59e4f0d94576502eef2f5818799f2db9.css?ver=d1918
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/litespeed/ucss/8a08b99bd17c5d702188cdc5490812b0.css?ver=d1918
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/litespeed/ucss/c9062085856c834a38b2cc78ed57756e.css?ver=d1918
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/litespeed/ucss/eac3fa6b870edd4da66db40179e2f5a1.css?ver=d1918
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/cookie-notice/css/front.min.css

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/cookie-notice/js/front.min.js
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/google-sitemap-generator/sitemap.xsl
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/en.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/ko.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/pl.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/gtranslate/js/base.js
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/image-carousel-divi/scripts/frontend-bundle.min.js
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/image-carousel-divi/styles/style.min.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/robo-gallery/cache/css/robo_gallery_css_id740_65022abaa4f71.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/robo-gallery/css/gallery.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/robo-gallery/includes/extensions/block/dist/blocks.style.build.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/robo-gallery/js/robo_gallery_alt.js
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/supreme-modules-for-divi/scripts/frontend-bundle.min.js
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/supreme-modules-for-divi/styles/style.min.css
Metody	GET
Atak	

Evidence	
Other Info	
URL	https://masiso.pl/wp-content/themes/Divi/core/admin/js/common.js
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/themes/Divi/core/admin/js/es6-promise.auto.min.js
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/themes/Divi/core/admin/js/recaptcha.js?ver=4.23.4
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/jquery.fitvids.js
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/magnific-popup.js
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/motion-effects.js
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/salvattore.js
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/themes/Divi/js/scripts.min.js
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/themes/masiso-theme-by-damian-popiol/ds-script.js
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/themes/masiso-theme-by-damian-popiol/style.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/bimbab-239x300.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/bimbab.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/bimbab.jpg.webp
Metody	GET
Atak	

Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/chicken-soup-239x300.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/chicken-soup.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/chicken-soup.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/chilli-chicken-239x300.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/chilli-chicken.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/chilli-chicken.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg
Metody	GET
Atak	
Evidence	
Other	

Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/chilli.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/cos.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/dragon-stroke.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/fale-pattern-grey.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/fale-pattern-orange.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/garlic.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/majeranek.svg

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/ornament-pattern-gey2.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/ornament-pattern-orange2.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/pattern-shape-189x300.png.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/pattern-shape.png
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/pattern-shape.png.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/05/roslina.svg
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/06/Kimchicabbage.Perfectasanadditiontodishesoreatenseparately_-480x320.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/06/Kimchicabbage.Perfectasanadditiontodishesoreatenseparately_-980x654.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/06/Kimchicabbage.Perfectasanadditiontodishesoreatenseparately_.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/06/Kimchicabbage.Perfectasanadditiontodishesoreatenseparately_.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/06/stars.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Clock.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi-1280x785.jpg.webp
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi-480x294.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi-980x601.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Dakgangjeong.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Direction.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/facebook.png
Metody	GET
Atak	

Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/google.png
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1-480x720.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1-682x1024.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1-682x1024.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-10-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other	

Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-10-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-10-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-10.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-15-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-15-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-15-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-15.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-16.jpg

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-19-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-19-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-19-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-19.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-1080x675.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-400x250.jpg
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-21-480x720.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-21.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-22-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-22-480x320.jpg
Metody	GET
Atak	
Evidence	

Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-22-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-22.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-25.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-27.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-28-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-28-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-28-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	

URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-28.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-30-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-30-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-30-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-30.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-31-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-31-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-31-980x653.jpg
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-31.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-32.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-33-480x720.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-33.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-34-480x720.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-34-480x720.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-34-682x1024.jpg
Metody	GET
Atak	

Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-34-682x1024.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-34.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-35-480x720.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-35.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-36.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-37-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-37-480x320.jpg
Metody	GET
Atak	
Evidence	
Other	

Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-37-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-37.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-38-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-38-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-38-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-38.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-4-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-4-480x320.jpg

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-4-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-4.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-6-480x720.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-6-480x720.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-6.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-6.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-1024x683.jpg
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-1280x854.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-480x320.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-980x654.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-980x654.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-1280x853.jpg
Metody	GET
Atak	
Evidence	

Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-1280x853.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-480x320.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-980x653.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	

URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-11.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-13.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-14-1280x853.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-14-480x320.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-14-980x653.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-14.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-14.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-15-1280x853.jpg.webp
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-15-480x320.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-15-980x653.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-15.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-15.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16-400x250.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16-480x720.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16-480x720.jpg.webp
Metody	GET
Atak	

Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16-933x675.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17-1280x853.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17-480x320.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17-980x653.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17.jpg
Metody	GET
Atak	
Evidence	
Other	

Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-1280x718.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-1280x718.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-480x269.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-480x269.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-980x550.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-980x550.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18.jpg

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-1280x853.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-480x320.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-980x653.jpg.webp
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-1280x852.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-1280x852.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-480x320.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-980x652.jpg
Metody	GET
Atak	
Evidence	

Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-980x652.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-1080x675.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-1280x853.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-400x250.jpg
Metody	GET
Atak	
Evidence	
Other Info	

URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-480x320.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-980x653.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-1024x574.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-1280x718.jpg.webp
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-480x269.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-480x269.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-980x550.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-980x550.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-22-1280x853.jpg
Metody	GET
Atak	

Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-22-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-22-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-22.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-3.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-4-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-4-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-4-980x653.jpg
Metody	GET
Atak	
Evidence	
Other	

Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-4.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-1280x853.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-480x320.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-980x653.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5.jpg

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6-1280x853.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6-1280x853.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6-480x320.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6-480x320.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6-980x653.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6-980x653.jpg.webp
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-1280x855.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-1280x855.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-480x321.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-480x321.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-980x655.jpg
Metody	GET
Atak	
Evidence	

Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-980x655.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Nagasaki-Czampong-1280x960.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Nagasaki-Czampong-480x360.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Nagasaki-Czampong-980x735.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/Nagasaki-Czampong.jpg
Metody	GET
Atak	
Evidence	
Other Info	

URL	https://masiso.pl/wp-content/uploads/2023/08/osam-bulgogi-480x640.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/osam-bulgogi.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/pyszne.png
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/08/tripadvisor.png
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/09/contact-ko.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/09/menu-ko.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/09/pyszne-ko.svg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2023/10/masiso-fav-icon.svg
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2024/01/Chefstirfryinwok-480x270.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2024/01/Chefstirfryinwok-980x551.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2024/01/Chefstirfryinwok.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2024/01/Chefstirfryinwok.jpg.webp
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/uploads/2024/01/TraditionalKoreanchickensoupwithhomemadenoodles-300x169.jpg
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/css/buttons.min.css?ver=6.4.2
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/css/dashicons.min.css?ver=6.4.2
Metody	GET
Atak	

Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/css/dist/block-editor/style.min.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/css/dist/block-library/style.min.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/css/dist/components/style.min.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/css/dist/editor/style.min.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/css/dist/patterns/style.min.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/css/dist/reusable-blocks/style.min.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/css/wp-embed-template-ie.min.css
Metody	GET
Atak	
Evidence	
Other	

Info	
URL	https://masiso.pl/wp-includes/js/dist/hooks.min.js?ver=c6aec9a8d4e5a5d543a1
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/js/dist/i18n.min.js?ver=7701b0c3857f914212ef
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.14.0
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/js/dist/vendor/wp-polyfill-inert.min.js?ver=3.1.2
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/js/jquery/jquery-migrate.min.js
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/js/jquery/jquery.min.js

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/js/jquery/jquery.min.js?ver=3.7.1
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/js/mediaelement/mediaelementplayer-legacy.min.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/js/mediaelement/wp-mediaelement.min.css
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/js/underscore.min.js?ver=1.13.4
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/js/wp-util.min.js?ver=6.4.2
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-includes/js/zxcvbn-async.min.js?ver=1.0
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fkontakt%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fmenu%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fo-restauracji%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fpolityka-prywatnosci%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2F

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fkontakt%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fmenu%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fo-restauracji%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fpolityka-prywatnosci%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/pages/21
Metody	GET
Atak	
Evidence	
Other Info	

URL	https://masiso.pl/wp-json/wp/v2/pages/24
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/pages/26
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/pages/28
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/pages/855
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/robogallery/740
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/users/1
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-login.php
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/xmlrpc.php
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/xmlrpc.php?rsd

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	

Evidence	
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	
Other Info	
Instances	390
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	https://masiso.pl
Metody	GET
Atak	
Evidence	1707943104
Other Info	1707943104, which evaluates to: 2024-02-14 21:38:24
URL	https://masiso.pl/
Metody	GET
Atak	
Evidence	1707943104
Other Info	1707943104, which evaluates to: 2024-02-14 21:38:24
URL	https://masiso.pl/?s
Metody	GET
Atak	
Evidence	1707943103
Other Info	1707943103, which evaluates to: 2024-02-14 21:38:23
URL	https://masiso.pl/author/damianpopiolgmail-com/
Metody	GET
Atak	
Evidence	1707943103

Other Info	1707943103, which evaluates to: 2024-02-14 21:38:23
URL	https://masiso.pl/gallery/740-2/feed/
Metody	GET
Atak	
Evidence	1707943103
Other Info	1707943103, which evaluates to: 2024-02-14 21:38:23
URL	https://masiso.pl/kontakt/
Metody	GET
Atak	
Evidence	1707943745
Other Info	1707943745, which evaluates to: 2024-02-14 21:49:05
URL	https://masiso.pl/kontakt/embed/
Metody	GET
Atak	
Evidence	1729289983
Other Info	1729289983, which evaluates to: 2024-10-19 00:19:43
URL	https://masiso.pl/menu/
Metody	GET
Atak	
Evidence	1707943605
Other Info	1707943605, which evaluates to: 2024-02-14 21:46:45
URL	https://masiso.pl/o-restauracji/
Metody	GET
Atak	
Evidence	1707943770
Other Info	1707943770, which evaluates to: 2024-02-14 21:49:30
URL	https://masiso.pl/page/2/?s
Metody	GET
Atak	
Evidence	1707943103
Other Info	1707943103, which evaluates to: 2024-02-14 21:38:23
URL	https://masiso.pl/polityka-prywatnosci/
Metody	GET
Atak	
Evidence	1708685896
Other Info	1708685896, which evaluates to: 2024-02-23 11:58:16

URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1416354905
Other Info	1416354905, which evaluates to: 2014-11-19 00:55:05
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1444681467
Other Info	1444681467, which evaluates to: 2015-10-12 22:24:27
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1473231341
Other Info	1473231341, which evaluates to: 2016-09-07 08:55:41
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1502002290
Other Info	1502002290, which evaluates to: 2017-08-06 08:51:30
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1518500249
Other Info	1518500249, which evaluates to: 2018-02-13 06:37:29
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1530992060
Other Info	1530992060, which evaluates to: 2018-07-07 21:34:20
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1560198380

Other Info	1560198380, which evaluates to: 2019-06-10 22:26:20
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1700485571
Other Info	1700485571, which evaluates to: 2023-11-20 14:06:11
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1732584193
Other Info	1732584193, which evaluates to: 2024-11-26 02:23:13
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1732584194
Other Info	1732584194, which evaluates to: 2024-11-26 02:23:14
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1735328473
Other Info	1735328473, which evaluates to: 2024-12-27 20:41:13
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1770035416
Other Info	1770035416, which evaluates to: 2026-02-02 13:30:16
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1804603682
Other Info	1804603682, which evaluates to: 2027-03-09 15:48:02
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET

Atak	
Evidence	1839030562
Other Info	1839030562, which evaluates to: 2028-04-11 03:49:22
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1859775393
Other Info	1859775393, which evaluates to: 2028-12-07 05:16:33
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1873313359
Other Info	1873313359, which evaluates to: 2029-05-12 22:49:19
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1894986606
Other Info	1894986606, which evaluates to: 2030-01-18 18:10:06
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1926607734
Other Info	1926607734, which evaluates to: 2031-01-19 17:48:54
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1958414417
Other Info	1958414417, which evaluates to: 2032-01-22 21:00:17
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	1990404162
Other Info	1990404162, which evaluates to: 2033-01-27 03:02:42

URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	2022574463
Other Info	2022574463, which evaluates to: 2034-02-03 11:14:23
URL	https://masiso.pl/wp-json/wp/v2/robogallery/740
Metody	GET
Atak	
Evidence	1696026743
Other Info	1696026743, which evaluates to: 2023-09-30 00:32:23
URL	https://masiso.pl/wp-json/wp/v2/users/1
Metody	GET
Atak	
Evidence	1708848904
Other Info	1708848904, which evaluates to: 2024-02-25 09:15:04
URL	https://masiso.pl/wp-json/wp/v2/users/1
Metody	GET
Atak	
Evidence	1708848905
Other Info	1708848905, which evaluates to: 2024-02-25 09:15:05
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	1707943102
Other Info	1707943102, which evaluates to: 2024-02-14 21:38:22
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	1707943104
Other Info	1707943104, which evaluates to: 2024-02-14 21:38:24
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	1707943102
Other Info	1707943102, which evaluates to: 2024-02-14 21:38:22
URL	https://masiso.pl/gallery/740-2/

Metody	POST
Atak	
Evidence	1709033283
Other Info	1709033283, which evaluates to: 2024-02-27 12:28:03
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	1707943745
Other Info	1707943745, which evaluates to: 2024-02-14 21:49:05
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	1707943604
Other Info	1707943604, which evaluates to: 2024-02-14 21:46:44
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	1707943605
Other Info	1707943605, which evaluates to: 2024-02-14 21:46:45
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	1707943770
Other Info	1707943770, which evaluates to: 2024-02-14 21:49:30
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	1707943102
Other Info	1707943102, which evaluates to: 2024-02-14 21:38:22
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	1708685896
Other Info	1708685896, which evaluates to: 2024-02-23 11:58:16
Instances	45
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://masiso.pl
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	https://masiso.pl/
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	https://masiso.pl/?s
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	https://masiso.pl/author/damianpopiolgmail-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	https://masiso.pl/author/damianpopiolgmail-com/feed/
Metody	GET
Atak	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	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://masiso.pl/comments/feed/
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	https://masiso.pl/feed/
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	https://masiso.pl/gallery/740-2/
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	https://masiso.pl/kontakt/
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	https://masiso.pl/kontakt/embed/
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	https://masiso.pl/menu/
Metody	GET
Atak	
Evidence	
Other	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

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://masiso.pl/menu/embed/
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	https://masiso.pl/o-restauracji/
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	https://masiso.pl/o-restauracji/embed/
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	https://masiso.pl/page-sitemap.html
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	https://masiso.pl/page-sitemap.xml
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	https://masiso.pl/page/2/?s
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	https://masiso.pl/polityka-prywatnosci/
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	https://masiso.pl/polityka-prywatnosci/embed/
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	https://masiso.pl/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.
URL	https://masiso.pl/search/feed/rss2/
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	https://masiso.pl/sitemap-misc.html
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	https://masiso.pl/sitemap-misc.xml
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	https://masiso.pl/sitemap.html
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	https://masiso.pl/sitemap.xml
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	https://masiso.pl/wp-admin/css/forms.min.css?ver=6.4.2
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	https://masiso.pl/wp-admin/css/l10n.min.css?ver=6.4.2
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	https://masiso.pl/wp-admin/css/login.min.css?ver=6.4.2
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	https://masiso.pl/wp-admin/js/password-strength-meter.min.js?ver=6.4.2
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	https://masiso.pl/wp-admin/js/user-profile.min.js?ver=6.4.2
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	https://masiso.pl/wp-content/et-cache/21/et-core-unified-21.min.css?ver=1707943102
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	https://masiso.pl/wp-content/et-cache/21/et-core-unified-tb-34-tb-53-deferred-21.min.css?ver=1707943104
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	https://masiso.pl/wp-content/et-cache/21/et-divi-dynamic-tb-34-tb-53-21-late.css
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	https://masiso.pl/wp-content/et-cache/21/et-divi-dynamic-tb-34-tb-53-21.css
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	https://masiso.pl/wp-content/et-cache/24/et-core-unified-24.min.css?ver=1707943604
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	https://masiso.pl/wp-content/et-cache/24/et-core-unified-tb-34-tb-53-deferred-24.min.css?ver=1707943605
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	https://masiso.pl/wp-content/et-cache/24/et-divi-dynamic-tb-34-tb-53-24-late.css
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	https://masiso.pl/wp-content/et-cache/24/et-divi-dynamic-tb-34-tb-53-24.css
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	https://masiso.pl/wp-content/et-cache/26/et-core-unified-26.min.css?ver=1707943770
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	https://masiso.pl/wp-content/et-cache/26/et-core-unified-tb-34-tb-53-deferred-26.min.css?ver=1707943770
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	https://masiso.pl/wp-content/et-cache/26/et-divi-dynamic-tb-34-tb-53-26-late.css
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	https://masiso.pl/wp-content/et-cache/26/et-divi-dynamic-tb-34-tb-53-26.css
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	https://masiso.pl/wp-content/et-cache/28/et-core-unified-28.min.css?ver=1707943745
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	https://masiso.pl/wp-content/et-cache/28/et-core-unified-tb-34-tb-53-deferred-28.min.css?ver=1707943745
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	https://masiso.pl/wp-content/et-cache/28/et-divi-dynamic-tb-34-tb-53-28-late.css
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	https://masiso.pl/wp-content/et-cache/28/et-divi-dynamic-tb-34-tb-53-28.css
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	https://masiso.pl/wp-content/et-cache/53/et-core-unified-cpt-deferred-53.min.css?ver=1707943103
Metody	GET
Atak	
Evidence	
Other	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

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://masiso.pl/wp-content/et-cache/740/et-divi-dynamic-tb-34-tb-53-740.css
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	https://masiso.pl/wp-content/et-cache/855/et-core-unified-tb-34-tb-53-deferred-855.min.css?ver=1708685896
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	https://masiso.pl/wp-content/et-cache/855/et-divi-dynamic-tb-34-tb-53-855-late.css
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	https://masiso.pl/wp-content/et-cache/855/et-divi-dynamic-tb-34-tb-53-855.css
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	https://masiso.pl/wp-content/et-cache/global/et-divi-customizer-global.min.css?ver=1707943102
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	https://masiso.pl/wp-content/et-cache/search/et-divi-dynamic-tb-34-tb-53-late.css
Metody	GET
Atak	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	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://masiso.pl/wp-content/et-cache/search/et-divi-dynamic-tb-34-tb-53.css
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	https://masiso.pl/wp-content/litespeed/css/e4115894001a031ae7109874cbde969d.css?ver=d1918
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	https://masiso.pl/wp-content/litespeed/css/e7c5e2684e7d3e9da278582d302fa5e5.css?ver=d1918
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	https://masiso.pl/wp-content/litespeed/ucss/192a8138017bf2a127a035a2f9e72d20.css?ver=d1918
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	https://masiso.pl/wp-content/litespeed/ucss/59e4f0d94576502eef2f5818799f2db9.css?ver=d1918
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	https://masiso.pl/wp-content/litespeed/ucss/8a08b99bd17c5d702188cdc5490812b0.css?ver=d1918
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	https://masiso.pl/wp-content/litespeed/ucss/c9062085856c834a38b2cc78ed57756e.css?ver=d1918
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	https://masiso.pl/wp-content/litespeed/ucss/eac3fa6b870edd4da66db40179e2f5a1.css?ver=d1918
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	https://masiso.pl/wp-content/plugins/cookie-notice/css/front.min.css
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	https://masiso.pl/wp-content/plugins/cookie-notice/js/front.min.js
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	https://masiso.pl/wp-content/plugins/google-sitemap-generator/sitemap.xsl
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	https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/en.svg

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	https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/ko.svg
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	https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/pl.svg
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	https://masiso.pl/wp-content/plugins/gtranslate/js/base.js
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	https://masiso.pl/wp-content/plugins/image-carousel-divi/scripts/frontend-bundle.min.js
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	https://masiso.pl/wp-content/plugins/image-carousel-divi/styles/style.min.css
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	https://masiso.pl/wp-content/plugins/robo-gallery/cache/css/robo_gallery_css_id740_65022abaa4f71.css

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	https://masiso.pl/wp-content/plugins/robo-gallery/css/gallery.css
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	https://masiso.pl/wp-content/plugins/robo-gallery/js/robo_gallery_alt.js
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	https://masiso.pl/wp-content/plugins/supreme-modules-for-divi/scripts/frontend-bundle.min.js
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	https://masiso.pl/wp-content/plugins/supreme-modules-for-divi/styles/style.min.css
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	https://masiso.pl/wp-content/themes/Divi/core/admin/js/common.js
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	https://masiso.pl/wp-content/themes/Divi/core/admin/js/es6-promise.auto.min.js
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	https://masiso.pl/wp-content/themes/Divi/core/admin/js/recaptcha.js?ver=4.23.4
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	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/jquery.fitvids.js
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	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/magnific-popup.js
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	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/motion-effects.js
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	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/salvattore.js
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	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
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	https://masiso.pl/wp-content/themes/Divi/js/scripts.min.js
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	https://masiso.pl/wp-content/themes/masiso-theme-by-damian-popiol/ds-script.js
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	https://masiso.pl/wp-content/themes/masiso-theme-by-damian-popiol/style.css
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	https://masiso.pl/wp-content/uploads/2023/05/bimbab-239x300.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/05/bimbab.jpg
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	https://masiso.pl/wp-content/uploads/2023/05/bimbab.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/05/chicken-soup-239x300.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/05/chicken-soup.jpg
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	https://masiso.pl/wp-content/uploads/2023/05/chicken-soup.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/05/chilli-chicken-239x300.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/05/chilli-chicken.jpg
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	https://masiso.pl/wp-content/uploads/2023/05/chilli-chicken.jpg.webp

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	https://masiso.pl/wp-content/uploads/2023/05/chilli-peczek.svg
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	https://masiso.pl/wp-content/uploads/2023/05/chilli.svg
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	https://masiso.pl/wp-content/uploads/2023/05/cos.svg
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	https://masiso.pl/wp-content/uploads/2023/05/dragon-fill.svg
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	https://masiso.pl/wp-content/uploads/2023/05/dragon-stroke.svg
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	https://masiso.pl/wp-content/uploads/2023/05/fale-pattern-grey.svg

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	https://masiso.pl/wp-content/uploads/2023/05/fale-pattern-orange.svg
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	https://masiso.pl/wp-content/uploads/2023/05/garlic.svg
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	https://masiso.pl/wp-content/uploads/2023/05/majeranek.svg
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	https://masiso.pl/wp-content/uploads/2023/05/masiso-logo-white.svg
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	https://masiso.pl/wp-content/uploads/2023/05/ornament-pattern-gey2.svg
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	https://masiso.pl/wp-content/uploads/2023/05/ornament-pattern-orange2.svg
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	https://masiso.pl/wp-content/uploads/2023/05/pattern-shape-189x300.png.webp
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	https://masiso.pl/wp-content/uploads/2023/05/pattern-shape.png
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	https://masiso.pl/wp-content/uploads/2023/05/pattern-shape.png.webp
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	https://masiso.pl/wp-content/uploads/2023/05/roslina.svg
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	https://masiso.pl/wp-content/uploads/2023/06/Kimchicabbage.Perfectasanadditiontodishesoreatenseparately_-480x320.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/06/Kimchicabbage.Perfectasanadditiontodishesoreatenseparately_-980x654.jpg.webp

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	https://masiso.pl/wp-content/uploads/2023/06/Kimchicabbage.Perfectasanadditiontodishesoreatenseparately_.jpg
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	https://masiso.pl/wp-content/uploads/2023/06/Kimchicabbage.Perfectasanadditiontodishesoreatenseparately_.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/06/stars.svg
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	https://masiso.pl/wp-content/uploads/2023/08/Clock.svg
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	https://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi-1280x785.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi-480x294.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi-980x601.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Dakgangjeong.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Direction.svg
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	https://masiso.pl/wp-content/uploads/2023/08/facebook.png

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	https://masiso.pl/wp-content/uploads/2023/08/google.png
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1-480x720.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1-682x1024.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1-682x1024.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1.jpg.webp

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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-10-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-10-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-10-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-10.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-15-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-15-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-15-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-15.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-16.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-19-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-19-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-19-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-19.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-1080x675.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-400x250.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-21-480x720.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-21.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-22-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-22-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-22-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-22.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-25.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-27.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-28-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-28-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-28-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-28.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-30-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-30-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-30-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-30.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-31-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-31-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-31-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-31.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-32.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-33-480x720.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-33.jpg
Metody	GET
Atak	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	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://masiso.pl/wp-content/uploads/2023/08/Masiso-34-480x720.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-34-480x720.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-34-682x1024.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-34-682x1024.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-34.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-35-480x720.jpg
Metody	GET
Atak	
Evidence	
Other	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

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-35.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-36.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-37-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-37-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-37-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-37.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-38-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-38-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-38-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-38.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-4-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-4-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-4-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-4.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-6-480x720.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-6-480x720.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-6.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-6.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-1024x683.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-1280x854.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-480x320.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-980x654.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-980x654.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1.jpg

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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-1280x853.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-480x320.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-980x653.jpg.webp

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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-11.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-13.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-14-1280x853.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-14-480x320.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-14-980x653.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-14.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-14.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-15-1280x853.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-15-480x320.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-15-980x653.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-15.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-15.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16-400x250.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16-480x720.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16-480x720.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16-933x675.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17-1280x853.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17-480x320.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17-980x653.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-1280x718.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-1280x718.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-480x269.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-480x269.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-980x550.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-980x550.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-1280x853.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-480x320.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-980x653.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-1280x852.jpg
Metody	GET
Atak	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	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://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-1280x852.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-480x320.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-980x652.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-980x652.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2.jpg
Metody	GET
Atak	
Evidence	
Other	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

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-1080x675.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-1280x853.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-400x250.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-480x320.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-980x653.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-1024x574.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-1280x718.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-480x269.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-480x269.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-980x550.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-980x550.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-22-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-22-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-22-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-22.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-3.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-4-1280x853.jpg

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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-4-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-4-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-4.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-1280x853.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-480x320.jpg

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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-480x320.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-980x653.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6-1280x853.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6-1280x853.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6-480x320.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6-480x320.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6-980x653.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6-980x653.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-1280x855.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-1280x855.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-480x321.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-480x321.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-980x655.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-980x655.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9.jpg.webp
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	https://masiso.pl/wp-content/uploads/2023/08/Nagasaki-Czampong-1280x960.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Nagasaki-Czampong-480x360.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Nagasaki-Czampong-980x735.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/Nagasaki-Czampong.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/osam-bulgogi-480x640.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/osam-bulgogi.jpg
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	https://masiso.pl/wp-content/uploads/2023/08/pyszne.png
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	https://masiso.pl/wp-content/uploads/2023/08/tripadvisor.png
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	https://masiso.pl/wp-content/uploads/2023/09/contact-ko.svg
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	https://masiso.pl/wp-content/uploads/2023/09/menu-ko.svg
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	https://masiso.pl/wp-content/uploads/2023/09/pyszne-ko.svg
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	https://masiso.pl/wp-content/uploads/2023/10/masiso-fav-icon.svg
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	https://masiso.pl/wp-content/uploads/2024/01/Chefstirfryinwok-480x270.jpg.webp
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	https://masiso.pl/wp-content/uploads/2024/01/Chefstirfryinwok-980x551.jpg.webp
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	https://masiso.pl/wp-content/uploads/2024/01/Chefstirfryinwok.jpg
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	https://masiso.pl/wp-content/uploads/2024/01/Chefstirfryinwok.jpg.webp
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	https://masiso.pl/wp-content/uploads/2024/01/TraditionalKoreanchickensoupwithhomemadenoodles-300x169.jpg
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	https://masiso.pl/wp-includes/css/buttons.min.css?ver=6.4.2
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	https://masiso.pl/wp-includes/css/dashicons.min.css?ver=6.4.2
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	https://masiso.pl/wp-includes/css/dist/block-editor/style.min.css
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	https://masiso.pl/wp-includes/css/dist/block-library/style.min.css
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	https://masiso.pl/wp-includes/css/dist/components/style.min.css
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	https://masiso.pl/wp-includes/css/dist/editor/style.min.css
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	https://masiso.pl/wp-includes/css/dist/patterns/style.min.css
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	https://masiso.pl/wp-includes/css/dist/reusable-blocks/style.min.css
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	https://masiso.pl/wp-includes/css/wp-embed-template-ie.min.css
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	https://masiso.pl/wp-includes/js/dist/hooks.min.js?ver=c6aec9a8d4e5a5d543a1
Metody	GET
Atak	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	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://masiso.pl/wp-includes/js/dist/i18n.min.js?ver=7701b0c3857f914212ef
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	https://masiso.pl/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.14.0
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	https://masiso.pl/wp-includes/js/dist/vendor/wp-polyfill-inert.min.js?ver=3.1.2
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	https://masiso.pl/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
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	https://masiso.pl/wp-includes/js/jquery/jquery-migrate.min.js
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	https://masiso.pl/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1
Metody	GET
Atak	
Evidence	
Other	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

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://masiso.pl/wp-includes/js/jquery/jquery.min.js
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	https://masiso.pl/wp-includes/js/jquery/jquery.min.js?ver=3.7.1
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	https://masiso.pl/wp-includes/js/mediaelement/mediaelementplayer-legacy.min.css
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	https://masiso.pl/wp-includes/js/mediaelement/wp-mediaelement.min.css
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	https://masiso.pl/wp-includes/js/underscore.min.js?ver=1.13.4
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	https://masiso.pl/wp-includes/js/wp-util.min.js?ver=6.4.2
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	https://masiso.pl/wp-includes/js/zxcvbn-async.min.js?ver=1.0
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	https://masiso.pl/wp-login.php
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	https://masiso.pl/wp-login.php?action=lostpassword
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	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
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	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
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	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	
Other	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

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
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	https://masiso.pl/wp-login.php?wp_lang=en_GB
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	https://masiso.pl/xmlrpc.php?rsd
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	https://masiso.pl/
Metody	POST
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	https://masiso.pl/gallery/740-2/
Metody	POST
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	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	
Other	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

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://masiso.pl/menu/
Metody	POST
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	https://masiso.pl/o-restauracji/
Metody	POST
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	https://masiso.pl/polityka-prywatnosci/
Metody	POST
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	https://masiso.pl/wp-login.php
Metody	POST
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	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
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	366
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.
	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx

Reference	https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informacyjny	**Charset Mismatch**
Opis	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set. An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2F
Metody	GET
Atak	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fkontakt%2F
Metody	GET
Atak	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fmenu%2F
Metody	GET
Atak	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fo-restauracji%2F
Metody	GET
Atak	
Evidence	
Other	There was a charset mismatch between the HTTP Header and the XML encoding

Info	declaration: [UTF-8] and [null] do not match.
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fpolityka-prywatnosci%2F
Metody	GET
Atak	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the XML encoding declaration: [UTF-8] and [null] do not match.
Instances	6
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	http://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id	436
WASC Id	15
Plugin Id	90011

Informacyjny	**Cookie Poisoning**
Opis	This check looks at user-supplied input in query string parameters and POST data to identify where cookie parameters might be controlled. This is called a cookie poisoning attack, and becomes exploitable when an attacker can manipulate the cookie in various ways. In some cases this will not be exploitable, however, allowing URL parameters to set cookie values is generally considered a bug.
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB User-input was found in the following cookie: wp_lang=en_GB; path=/; secure The user input was: wp_lang=en_GB
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB User-input was found in the following cookie: wp_lang=en_GB; path=/; secure The user input was: wp_lang=en_GB
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	An attacker may be able to poison cookie values through URL parameters. Try injecting a semicolon to see if you can add cookie values (e.g. name=controlledValue; name=anotherValue;). This was identified at: https://masiso.pl/wp-login.php?wp_lang=en_GB User-input was found in the following cookie: wp_lang=en_GB; path=/; secure The user input was: wp_lang=en_GB

Instances	3
Solution	Do not allow user input to control cookie names and values. If some query string parameters must be set in cookie values, be sure to filter out semicolon's that can serve as name/value pair delimiters.
Reference	http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-cookie
CWE Id	565
WASC Id	20
Plugin Id	10029

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	https://masiso.pl
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script id="divi-custom-script-js-extra" type="litespeed/javascript">var DIVI= {"item_count":"%d Item","items_count":"%d Items"};", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script id="divi-custom-script-js-extra" type="litespeed/javascript">var DIVI= {"item_count":"%d Item","items_count":"%d Items"};", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/?s
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script async id="cookie-notice-front-js-before" type="litespeed /javascript">var cnArgs={"ajaxUrl":"https:\/\/masiso.pl\/wp-admi", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/author/damianpopiolgmail-com/
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script async id="cookie-notice-front-js-before" type="litespeed /javascript">var cnArgs={"ajaxUrl":"https:\/\/masiso.pl\/wp-admi", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/gallery/740-2/
Metody	GET
Atak	
Evidence	admin

Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script async id="cookie-notice-front-js-before" type="litespeed /javascript">var cnArgs={"ajaxUrl":"https:\/\/masiso.pl\/wp-admi", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/gallery/740-2/feed/
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script async id="cookie-notice-front-js-before" type="litespeed /javascript">var cnArgs={"ajaxUrl":"https:\/\/masiso.pl\/wp-admi", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/kontakt/
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script id="divi-custom-script-js-extra" type="litespeed/javascript">var DIVI= {"item_count":"%d Item","items_count":"%d Items"};", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/kontakt/embed/
Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> /* <![CDATA[*/ /*! This file is auto-generated */ !function(c,u) {"use strict";var r,t,e,a=u.que", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/menu/
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script id="divi-custom-script-js-extra" type="litespeed/javascript">var DIVI= {"item_count":"%d Item","items_count":"%d Items"};", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/menu/embed/
Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> /* <![CDATA[*/ /*! This file is auto-generated */ !function(c,u) {"use strict";var r,t,e,a=u.que", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/o-restauracji/
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script id="divi-custom-script-js-extra" type="litespeed/javascript">var DIVI= {"item_count":"%d Item","items_count":"%d Items"};", see evidence field for the suspicious

	comment/snippet.
URL	https://masiso.pl/o-restauracji/embed/
Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> /* <![CDATA[*/ /*! This file is auto-generated */ !function(c,u) {"use strict";var r,t,e,a=u.que", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/page/2/?s
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script async id="cookie-notice-front-js-before" type="litespeed /javascript">var cnArgs={"ajaxUrl":"https:\/\/masiso.pl\/wp-admi", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/polityka-prywatnosci/
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 2 times, the first in the element starting with: "<script async id="cookie-notice-front-js-before" type="litespeed /javascript">var cnArgs={"ajaxUrl":"https:\/\/masiso.pl\/wp-admi", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/polityka-prywatnosci/embed/
Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> /* <![CDATA[*/ /*! This file is auto-generated */ !function(c,u) {"use strict";var r,t,e,a=u.que", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-admin/js/user-profile.min.js?ver=6.4.2
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "! function(o){var e,a,t,n,i,r,p,d,l,c,u=!1,h=wp.i18n.__;function f(){"function"!=typeof zxcvbn? setTimeout(f,50):(!a.val()||c.hasC", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-content/plugins/gtranslate/js/base.js
Metody	GET
Atak	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: " var u_class = '.gt_raw_link-'+Array.from('base'+wrapper_selector).reduce(function(h,c) {return 0|(31*h+c.charCodeAt(0))},0).t", see evidence field for the suspicious comment /snippet.
URL	https://masiso.pl/wp-content/plugins/gtranslate/js/base.js

Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: " window.doGTranslate = function(lang_pair){if(lang_pair.value)lang_pair=lang_pair.value;if (lang_pair==")return;var lang=", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-content/plugins/image-carousel-divi/scripts/frontend-bundle.min.js
Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "!function(i){var e={};function t(o){if(e[o])return e[o].exports;var s=e[o]={i:o,l:!1,exports:{}}; return i[o].call(s.exports,s,s.", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-content/plugins/robo-gallery/js/robo_gallery_alt.js
Metody	GET
Atak	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected 2 times, the first in the element starting with: "(function(){function e(){}function t(e,t){for(var n=e.length;n--;)if(e[n]. listener===t)return n;return-1}function n(e){return fu", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-content/plugins/robo-gallery/js/robo_gallery_alt.js
Metody	GET
Atak	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 2 times, the first in the element starting with: "var BaseEffect=function(c,h){function e(){}return((e.prototype=Object. create(roboEffectClass)).constructor=e).prototype.addEffec", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-content/plugins/robo-gallery/js/robo_gallery_alt.js
Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "!function(e){"function"==typeof define&&define.amd&&define.amd.jQuery?define(["jquery"], e):"undefined"!=typeof module&&module.ex", see evidence field for the suspicious comment /snippet.
URL	https://masiso.pl/wp-content/plugins/robo-gallery/js/robo_gallery_alt.js
Metody	GET
Atak	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "function(n){function f(e,t,n){var r="0x"+t-65536;return r!=r||n?t:r<0?String. fromCharCode(65536+r):String.fromCharCode(r>>10|552", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-content/themes/Divi/core/admin/js/common.js
Metody	GET
Atak	

Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 2 times, the first in the element starting with: " // use navigator.appName as browser name if we were unable to get it from user_agent", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/magnific-popup.js
Metody	GET
Atak	
Evidence	FROM
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/motion-effects.js
Metody	GET
Atak	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected in the element starting with: "!function(t){var e={};function r(n){if(e[n])return e[n].exports;var o=e[n]={i:n,l:!1,exports:{}}; return t[n].call(o.exports,o,o.", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/salvattore.js
Metody	GET
Atak	
Evidence	FROM
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/salvattore.js
Metody	GET
Atak	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "!function(e,t){"function"==typeof define&&define.amd?define([],t):"object"==typeof exports? module.exports=t():e.salvattore=t()}(", see evidence field for the suspicious comment /snippet.
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected in the element starting with: "!function(t){var e={};function n(r){if(e[r])return e[r].exports;var o=e[r]={i:r,l:!1,exports:{}}; return t[r].call(o.exports,o,o.", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-content/themes/Divi/js/scripts.min.js
Metody	GET
Atak	
Evidence	db

Other Info	The following pattern was used: \bDB\b and was detected in the element starting with: "!function(t){var e={};function n(i){if(e[i])return e[i].exports;var a=e[i]={i:i,l:!1,exports:{}};return t[i].call(a.exports,a,a.", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-includes/js/dist/vendor/wp-polyfill-inert.min.js?ver=3.1.2
Metody	GET
Atak	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "!function(e){"object"==typeof exports&&"undefined"!=typeof module||"function"!=typeof define||!define.amd?e():define("inert",e)}", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-includes/js/dist/vendor/wp-polyfill.min.js?ver=3.15.0
Metody	GET
Atak	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "!function(t){"use strict";var r,e,n;e={},(n=function(t){if(e[t])return e[t].exports;var o=e[t]={i:t,l:!1,exports:{}};return r[t]", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-includes/js/jquery/jquery-migrate.min.js
Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: ""undefined"==typeof jQuery.migrateMute&&(jQuery.migrateMute=!0),function(t){"use strict";"function"==typeof define&&define.amd?d", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1
Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: ""undefined"==typeof jQuery.migrateMute&&(jQuery.migrateMute=!0),function(t){"use strict";"function"==typeof define&&define.amd?d", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-includes/js/jquery/jquery.min.js
Metody	GET
Atak	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-includes/js/jquery/jquery.min.js?ver=3.7.1
Metody	GET
Atak	
Evidence	username
Other	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?

Info	module.exports=e.document?t(e,!0):function(", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-includes/js/underscore.min.js?ver=1.13.4
Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "!function(n,r){var t,e;"object"==typeof exports&&"undefined"!=typeof module?module.exports=r():"function"==typeof define&&define", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-includes/js/wp-util.min.js?ver=6.4.2
Metody	GET
Atak	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "window.wp=window.wp||{},function(s){var t="undefined"==typeof _wpUtilSettings?{}:_wpUtilSettings;wp.template=_.memoize(function(", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-login.php
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script type="text/javascript" id="password-strength-meter-js-translations"> /* <![CDATA[*/ (function(domain, translations) ", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-login.php
Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> /* <![CDATA[*/ function wp_attempt_focus() {setTimeout(function() {try {d = document.getElemen", see evidence field for the suspicious comment /snippet.
URL	https://masiso.pl/wp-login.php
Metody	GET
Atak	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script type="text/javascript" id="user-profile-js-extra"> /* <![CDATA[*/ var userProfileL10n = {"user_id":"0","nonce":"956930b", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script type="text/javascript" id="password-strength-meter-js-translations"> /* <![CDATA[*/ (function(domain, translations) ", see evidence field for the

	suspicious comment/snippet.
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> /* <![CDATA[*/ function wp_attempt_focus() {setTimeout(function() {try {d = document.getElemen", see evidence field for the suspicious comment /snippet.
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script type="text/javascript" id="user-profile-js-extra"> /* <![CDATA[*/ var userProfileL10n = {"user_id":"0","nonce":"956930b", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script type="text/javascript" id="password-strength-meter-js-translations"> /* <![CDATA[*/ (function(domain, translations) ", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> /* <![CDATA[*/ function wp_attempt_focus() {setTimeout(function() {try {d = document.getElemen", see evidence field for the suspicious comment /snippet.
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script type="text/javascript" id="user-profile-js-extra"> /* <![CDATA[*/ var userProfileL10n = {"user_id":"0","nonce":"956930b", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	admin

Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script type="text/javascript" id="password-strength-meter-js-translations"> /* <![CDATA[*/ (function(domain, translations) ", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> /* <![CDATA[*/ function wp_attempt_focus() {setTimeout(function() {try {d = document.getElemen", see evidence field for the suspicious comment /snippet.
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script type="text/javascript" id="user-profile-js-extra"> /* <![CDATA[*/ var userProfileL10n = {"user_id":"0","nonce":"956930b", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script type="text/javascript" id="password-strength-meter-js-translations"> /* <![CDATA[*/ (function(domain, translations) ", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> /* <![CDATA[*/ function wp_attempt_focus() {setTimeout(function() {try {d = document.getElemen", see evidence field for the suspicious comment /snippet.
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script type="text/javascript" id="user-profile-js-extra"> /* <![CDATA[*/ var userProfileL10n = {"user_id":"0","nonce":"956930b", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	admin
	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the

Other Info	element starting with: "<script async type="text/javascript" id="cookie-notice-front-js-before" > /* <![CDATA[*/ var cnArgs = {"ajaxUrl":"https:\/\/masi", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script async type="text/javascript" id="cookie-notice-front-js-before" > /* <![CDATA[*/ var cnArgs = {"ajaxUrl":"https:\/\/masi", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script async type="text/javascript" id="cookie-notice-front-js-before" > /* <![CDATA[*/ var cnArgs = {"ajaxUrl":"https:\/\/masi", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script async type="text/javascript" id="cookie-notice-front-js-before" > /* <![CDATA[*/ var cnArgs = {"ajaxUrl":"https:\/\/masi", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script async type="text/javascript" id="cookie-notice-front-js-before" > /* <![CDATA[*/ var cnArgs = {"ajaxUrl":"https:\/\/masi", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script async type="text/javascript" id="cookie-notice-front-js-before" > /* <![CDATA[*/ var cnArgs = {"ajaxUrl":"https:\/\/masi", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	admin
Other	The following pattern was used: \bADMIN\b and was detected 5 times, the first in the element starting with: "<script type="text/javascript" id="password-strength-meter-js-

Info	translations"> /* <![CDATA[*/ (function(domain, translations) ", see evidence field for the suspicious comment/snippet.
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script type="text/javascript"> /* <![CDATA[*/ function wp_attempt_focus() {setTimeout(function() {try {d = document.getElemen", see evidence field for the suspicious comment /snippet.
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: "<script type="text/javascript" id="user-profile-js-extra"> /* <![CDATA[*/ var userProfileL10n = {"user_id":"0","nonce":"956930b", see evidence field for the suspicious comment/snippet.
Instances	62
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
URL	https://masiso.pl
Metody	GET
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img data-lazyloaded="1" src= PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIxNiIgaGVpZ decoding="async" data-src="https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/pl.svg" wi
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/
Metody	GET
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img data-lazyloaded="1" src= PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIxNiIgaGVpZ decoding="async" data-src="https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/pl.svg" wi
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/?s
Metody	GET
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img decoding="async" src="h

Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/author/damianpopiolgmail-com/
Metody	GET
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img data-lazyloaded="1" src= PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIxNiIgaGVpZ decoding="async" data-src="https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/pl.svg" wi
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/gallery/740-2/
Metody	GET
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img data-lazyloaded="1" src= PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIxNiIgaGVpZ decoding="async" data-src="https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/pl.svg" wi
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/gallery/740-2/feed/
Metody	GET
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img data-lazyloaded="1" src= PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIxNiIgaGVpZ decoding="async" data-src="https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/pl.svg" wi
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/kontakt/
Metody	GET
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img data-lazyloaded="1" src= PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIxNiIgaGVpZ decoding="async" data-src="https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/pl.svg" wi
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/menu/
Metody	GET
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img data-lazyloaded="1" src= PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIxNiIgaGVpZ decoding="async" data-src="https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/pl.svg" wi
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/o-restauracji/
Metody	GET
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img data-lazyloaded="1" src= PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIxNiIgaGVpZ decoding="async" data-src="https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/pl.svg" wi
Other	

Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/page/2/?s
Metody	GET
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img decoding="async" src="h
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/polityka-prywatnosci/
Metody	GET
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img data-lazyloaded="1" src= PHN2ZyB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHdpZHRoPSIxNiIgaGVpZ decoding="async" data-src="https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/pl.svg" wi
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img decoding="async" src="h
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img decoding="async" src="h
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img decoding="async" src="h
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img decoding="async" src="h
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img decoding="async" src="h
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this

URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	<a href="#" data-gt-lang="pl" class="gt-current-lang notranslate"><img decoding="async" src="h
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
Instances	17
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://masiso.pl
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/?s
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/author/damianpopiolgmail-com/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/author/damianpopiolgmail-com/feed/
Metody	GET
Atak	

Evidence	
Other Info	
URL	https://masiso.pl/comments/feed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/feed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/gallery/740-2/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/kontakt/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/kontakt/embed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/menu/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/menu/embed/
Metody	GET
Atak	
Evidence	
Other	

Info	
URL	https://masiso.pl/o-restauracji/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/o-restauracji/embed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/page-sitemap.html
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/page-sitemap.xml
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/page/2/?s
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/embed/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/robots.txt

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/search/feed/rss2/
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/sitemap-misc.html
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/sitemap-misc.xml
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/sitemap.html
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/sitemap.xml
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-content/plugins/google-sitemap-generator/sitemap.xsl
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/
Metody	GET

Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fkontakt%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fmenu%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fo-restauracji%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fpolityka-prywatnosci%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2F

Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fkontakt%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fmenu%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fo-restauracji%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fpolityka-prywatnosci%2F
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/pages/21
Metody	GET
Atak	
Evidence	
Other Info	

URL	https://masiso.pl/wp-json/wp/v2/pages/24
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/pages/26
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/pages/28
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/pages/855
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/robogallery/740
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-json/wp/v2/users/1
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-login.php
Metody	GET
Atak	
Evidence	no-cache, must-revalidate, max-age=0
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword

Metody	GET
Atak	
Evidence	no-cache, must-revalidate, max-age=0
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	no-cache, must-revalidate, max-age=0
Other Info	
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	no-cache, must-revalidate, max-age=0
Other Info	
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	no-cache, must-revalidate, max-age=0
Other Info	
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	no-cache, must-revalidate, max-age=0
Other Info	
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	no-cache, must-revalidate, max-age=0
Other Info	
URL	https://masiso.pl/xmlrpc.php?rsd
Metody	GET
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/

Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	
Other Info	
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	no-cache, must-revalidate, max-age=0
Other Info	
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	

Evidence	no-cache, must-revalidate, max-age=0
Other Info	
Instances	62
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	**Retrieved from Cache**
Opis	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://masiso.pl/robots.txt
Metody	GET
Atak	
Evidence	Age: 496
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2.jpg
Metody	GET
Atak	
Evidence	Age: 547
Other Info	The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use.
Instances	2
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 http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
CWE Id	

WASC Id	
Plugin Id	10050

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	https://masiso.pl/wp-login.php
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other	

Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/?p=855
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/author/damianpopiolgmail-com/feed
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/gallery/740-2
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/gallery/740-2
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/gallery/740-2/feed

Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/gallery/740-2/feed
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/menu/embed
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/o-restauracji/embed
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/page-sitemap.html
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/page/2
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/page/2
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/page/2/?s
Metody	GET

Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/polityka-prywatnosci/embed
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/polityka-prywatnosci/embed
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/polityka-prywatnosci/embed/
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/search/feed/rss2
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/search/feed/rss2
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/sitemap-misc.html
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/sitemap.html
Metody	GET
Atak	
Evidence	WP%20Cookie%20check

Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-admin/css
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-admin/js
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-admin/js/user-profile.min.js?ver=6.4.2
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/et-cache/24/et-core-unified-tb-34-tb-53-deferred-24.min.css?ver=1707943605
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/et-cache/28/et-core-unified-28.min.css?ver=1707943745
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/et-cache/53/et-core-unified-cpt-deferred-53.min.css?ver=1707943103
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/et-cache/740
Metody	GET
Atak	
Evidence	WP%20Cookie%20check

Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/et-cache/740/et-divi-dynamic-tb-34-tb-53-740.css
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/et-cache/855
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/et-cache/855/et-divi-dynamic-tb-34-tb-53-855.css
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/et-cache/global
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/et-cache/global/et-divi-customizer-global.min.css?ver=1707943102
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/et-cache/search
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/et-cache/search/et-divi-dynamic-tb-34-tb-53-late.css
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai

URL	https://masiso.pl/wp-content/et-cache/search/et-divi-dynamic-tb-34-tb-53-late.css
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/litespeed/css
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/litespeed/css
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/litespeed/css/e7c5e2684e7d3e9da278582d302fa5e5.css?ver=d1918
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/litespeed/css/e7c5e2684e7d3e9da278582d302fa5e5.css?ver=d1918
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/litespeed/ucss/59e4f0d94576502eef2f5818799f2db9.css?ver=d1918
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/litespeed/ucss/8a08b99bd17c5d702188cdc5490812b0.css?ver=d1918
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other	

Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/plugins/cookie-notice/js
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/plugins/gtranslate/flags/svg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/plugins/gtranslate/flags/svg/ko.svg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/plugins/image-carousel-divi
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/plugins/robo-gallery/cache/css
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/plugins/robo-gallery/cache/css /robo_gallery_css_id740_65022abaa4f71.css
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/plugins/robo-gallery/js/robo_gallery_alt.js
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie

URL	https://masiso.pl/wp-content/plugins/supreme-modules-for-divi/scripts/frontend-bundle.min.js
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/themes/Divi/core
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/themes/Divi/core/admin/js/common.js
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/themes/Divi/core/admin/js/es6-promise.auto.min.js
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/salvattore.js
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/themes/Divi/includes/builder/feature/dynamic-assets/assets/js/sticky-elements.js
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/themes/masiso-theme-by-damian-popiol/style.css
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/05

Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/05/chicken-soup-239x300.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/05/chilli-chicken-239x300.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/05/chilli.svg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/05/cos.svg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/05/cos.svg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/05/pattern-shape-189x300.png.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/05/pattern-shape.png
Metody	GET

Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/05/pattern-shape.png.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/05/roslina.svg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/05/roslina.svg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/06
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/06/stars.svg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/06/stars.svg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi-480x294.jpg.webp
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE

Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi-480x294.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Daeji-Bulgogi.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/facebook.png
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1-480x720.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1-682x1024.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1-682x1024.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1-682x1024.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie

URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-1.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-10-480x320.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-10-980x653.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-15-480x320.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-19-1280x853.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-19-480x320.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-19-480x320.jpg
Metody	GET

Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-19-980x653.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-1080x675.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-1080x675.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-400x250.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-400x250.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-980x653.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-2-980x653.jpg
Metody	GET
Atak	

Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-22-480x320.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-22-980x653.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-25.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-27.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-28-1280x853.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-28-480x320.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-28-480x320.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other	

Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-30-1280x853.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-31-980x653.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-33-480x720.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-34-480x720.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-34-480x720.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-34-682x1024.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-36.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-37-980x653.jpg

Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-37-980x653.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-38-1280x853.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-6-480x720.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-6.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-1024x683.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-1024x683.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-480x320.jpg
Metody	GET

Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-480x320.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-980x654.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-1-980x654.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-1280x853.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-980x653.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10-980x653.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-10.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check

Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-14-980x653.jpg.webp
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-15-480x320.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16-480x720.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16-480x720.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16-933x675.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16-933x675.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-16.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie

URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17-1280x853.jpg.webp
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-17.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-1280x718.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-1280x718.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-1280x718.jpg.webp
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-1280x718.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-480x269.jpg
Metody	GET

Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18-480x269.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-18.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-1280x853.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-480x320.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-19-980x653.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-1280x852.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-1280x852.jpg.webp
Metody	GET
Atak	

Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-2-980x652.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-1080x675.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-1080x675.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-1280x853.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-1280x853.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-480x320.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-480x320.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other	

Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-20-980x653.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-480x269.jpg.webp
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21-980x550.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-21.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-22-1280x853.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-3.jpg

Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-3.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-4-1280x853.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-4-980x653.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-1280x853.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-480x320.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-480x320.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-980x653.jpg
Metody	GET

Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5-980x653.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-5.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6-480x320.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6-980x653.jpg.webp
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-6.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-1280x855.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-980x655.jpg.webp
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE

Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Masiso-produkty-9-980x655.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Nagasaki-Czampong-1280x960.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Nagasaki-Czampong-1280x960.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/Nagasaki-Czampong-980x735.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/08/Nagasaki-Czampong-980x735.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/08/tripadvisor.png
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2023/09
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai

URL	https://masiso.pl/wp-content/uploads/2023/09/menu-ko.svg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2023/09/menu-ko.svg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2024/01
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2024/01/Chefstirfryinwok.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2024/01/Chefstirfryinwok.jpg.webp
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-content/uploads/2024/01 /TraditionalKoreanchickensoupwithhomemadenoodles-300x169.jpg
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-content/uploads/2024/01 /TraditionalKoreanchickensoupwithhomemadenoodles-300x169.jpg
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-includes/css/dashicons.min.css?ver=6.4.2

Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-includes/css/dist/patterns
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-includes/css/wp-embed-template-ie.min.css
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-includes/css/wp-embed-template-ie.min.css
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-includes/js/dist/hooks.min.js?ver=c6aec9a8d4e5a5d543a1
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-includes/js/dist/vendor/regenerator-runtime.min.js?ver=0.14.0
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-includes/js/jquery
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-includes/js/jquery/jquery-migrate.min.js?ver=3.4.1
Metody	GET

Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-includes/js/underscore.min.js?ver=1.13.4
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-json/oembed/1.0/embed?format=xml&url=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-json/oembed/1.0/embed?url=https%3A%2F%2Fmasiso.pl%2Fpolityka-prywatnosci%2F
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-json/wp/v2/robogallery
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-json/wp/v2/users
Metody	GET

Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-login.php
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/wp-login.php
Metody	GET
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	jetpack%3AzKIPGf7y%2FakKKfh4tzvrQ2BE
Other Info	cookie:tk_ai
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	WP%20Cookie%20check
Other Info	cookie:wordpress_test_cookie
Instances	215
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

Informacyjny	**User Controllable HTML Element Attribute (Potential XSS)**
Opis	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?action=lostpassword appears to include user input in: a(n) [form] tag [id] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?action=lostpassword appears to include user input in: a(n) [form] tag [name] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?action=lostpassword appears to include user input in: a(n) [input] tag [value] attribute The user input found was: action=lostpassword The user-controlled value was: lostpassword
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB appears to include user input in: a(n) [form] tag [id] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?

Info	action=lostpassword&wp_lang=en_GB appears to include user input in: a(n) [form] tag [name] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB appears to include user input in: a(n) [input] tag [value] attribute The user input found was: action=lostpassword The user-controlled value was: lostpassword
URL	https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?action=lostpassword&wp_lang=en_GB appears to include user input in: a(n) [option] tag [value] attribute The user input found was: wp_lang=en_GB The user-controlled value was: en_gb
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/

URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/css/forms.min.css?ver=6.4.2
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/css/l10n.min.css?ver=6.4.2
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/css/login.min.css?ver=6.4.2
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/js/password-strength-meter.min.js?ver=6.4.2
URL	https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?reauth=1&redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F appears to include user input in: a(n) [script] tag [src] attribute The user input found was:

	redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/js/user-profile.min.js?ver=6.4.2
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/gallery/740-2/ The user-controlled value was: https://masiso.pl
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/gallery/740-2/ The user-controlled value was: https://masiso.pl/
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fgallery%2F740-2%2F appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=https://masiso.pl/gallery/740-2/ The user-controlled value was: https://masiso.pl/gallery/740-2/
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?

Info	redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/css/forms.min.css?ver=6.4.2
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/css/l10n.min.css?ver=6.4.2
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/css/login.min.css?ver=6.4.2
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	

Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/js/password-strength-meter.min.js?ver=6.4.2
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/js/user-profile.min.js?ver=6.4.2
URL	https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?redirect_to=https%3A%2F%2Fmasiso.pl%2Fwp-admin%2F&wp_lang=en_GB appears to include user input in: a(n) [option] tag [value] attribute The user input found was: wp_lang=en_GB The user-controlled value was: en_gb
URL	https://masiso.pl/wp-login.php?wp_lang=en_GB
Metody	GET
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?wp_lang=en_GB appears to include user input in: a(n) [option] tag [value] attribute The user input found was: wp_lang=en_GB The user-controlled value was: en_gb
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpnonce-et-pb-contact-form-submitted-0=9e1ce563fe The user-controlled value was: 9e1ce563fe
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contact_email_0=ZAP The user-controlled value was: zap

URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contact_nazwa_rezerwacji_0=ZAP The user-controlled value was: zap
URL	https://masiso.pl/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contactform_submit_0=et_contact_proccess The user-controlled value was: et_contact_proccess
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/gallery/740-2/ appears to include user input in: a(n) [a] tag [href] attribute The user input found was: _wp_http_referer=/gallery/740-2/ The user-controlled value was: /gallery/740-2/#respond
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/gallery/740-2/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wp_http_referer=/gallery/740-2/ The user-controlled value was: /gallery/740-2/
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/gallery/740-2/ appears to include user input in: a(n) [script] tag [data-gt-orig-url] attribute The user input found was: _wp_http_referer=/gallery/740-2/ The user-controlled value was: /gallery/740-2/
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	
Other	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/gallery/740-2/

Info	appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpnonce-et-pb-contact-form-submitted-0=9e1ce563fe The user-controlled value was: 9e1ce563fe
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/gallery/740-2/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contact_email_0=ZAP The user-controlled value was: zap
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/gallery/740-2/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contact_nazwa_rezerwacji_0=ZAP The user-controlled value was: zap
URL	https://masiso.pl/gallery/740-2/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/gallery/740-2/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contactform_submit_0=et_contact_proccess The user-controlled value was: et_contact_proccess
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/kontakt/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wp_http_referer=/kontakt/ The user-controlled value was: /kontakt/
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/kontakt/ appears to include user input in: a(n) [script] tag [data-gt-orig-url] attribute The user input found was: _wp_http_referer=/kontakt/ The user-controlled value was: /kontakt/
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: https://masiso.pl/kontakt/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpnonce-et-pb-contact-form-submitted-0=9e1ce563fe The user-controlled value was: 9e1ce563fe
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/kontakt/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contact_email_0=ZAP The user-controlled value was: zap
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/kontakt/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contact_nazwa_rezerwacji_0=ZAP The user-controlled value was: zap
URL	https://masiso.pl/kontakt/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/kontakt/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contactform_submit_0=et_contact_proccess The user-controlled value was: et_contact_proccess
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/menu/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wp_http_referer=/menu/ The user-controlled value was: /menu/
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/menu/ appears to include user input in: a(n) [script] tag [data-gt-orig-url] attribute The user input found was: _wp_http_referer=/menu/ The user-controlled value was: /menu/
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: https://masiso.pl/menu/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpnonce-et-pb-contact-form-submitted-0=9e1ce563fe The user-controlled value was: 9e1ce563fe
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/menu/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contact_email_0=ZAP The user-controlled value was: zap
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/menu/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contact_nazwa_rezerwacji_0=ZAP The user-controlled value was: zap
URL	https://masiso.pl/menu/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/menu/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contactform_submit_0=et_contact_proccess The user-controlled value was: et_contact_proccess
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/o-restauracji/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wp_http_referer=/o-restauracji/ The user-controlled value was: /o-restauracji/
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/o-restauracji/ appears to include user input in: a(n) [script] tag [data-gt-orig-url] attribute The user input found was: _wp_http_referer=/o-restauracji/ The user-controlled value was: /o-restauracji/
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	
	User-controlled HTML attribute values were found. Try injecting special characters to see if

Other Info	XSS might be possible. The page at the following URL: https://masiso.pl/o-restauracji/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpnonce-et-pb-contact-form-submitted-0=9e1ce563fe The user-controlled value was: 9e1ce563fe
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/o-restauracji/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contact_email_0=ZAP The user-controlled value was: zap
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/o-restauracji/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contact_nazwa_rezerwacji_0=ZAP The user-controlled value was: zap
URL	https://masiso.pl/o-restauracji/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/o-restauracji/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contactform_submit_0=et_contact_proccess The user-controlled value was: et_contact_proccess
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/polityka-prywatnosci/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wp_http_referer=/polityka-prywatnosci/ The user-controlled value was: /polityka-prywatnosci/
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/polityka-prywatnosci/ appears to include user input in: a(n) [script] tag [data-gt-orig-url] attribute The user input found was: _wp_http_referer=/polityka-prywatnosci/ The user-controlled value was: /polityka-prywatnosci/
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	

Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/polityka-prywatnosci/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _wpnonce-et-pb-contact-form-submitted-0=9e1ce563fe The user-controlled value was: 9e1ce563fe
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/polityka-prywatnosci/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contact_email_0=ZAP The user-controlled value was: zap
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/polityka-prywatnosci/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contact_nazwa_rezerwacji_0=ZAP The user-controlled value was: zap
URL	https://masiso.pl/polityka-prywatnosci/
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/polityka-prywatnosci/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: et_pb_contactform_submit_0=et_contact_proccess The user-controlled value was: et_contact_proccess
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php appears to include user input in: a(n) [a] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/
URL	https://masiso.pl/wp-login.php
Metody	POST

Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/css/forms.min.css?ver=6.4.2
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/css/l10n.min.css?ver=6.4.2
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php appears to include user input in: a(n) [link] tag [href] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/css/login.min.css?ver=6.4.2
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was: redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/js/password-strength-meter.min.js?ver=6.4.2
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	
Other	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php appears to include user input in: a(n) [script] tag [src] attribute The user input found was:

Info	redirect_to=https://masiso.pl/wp-admin/ The user-controlled value was: https://masiso.pl/wp-admin/js/user-profile.min.js?ver=6.4.2
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: rememberme=forever The user-controlled value was: forever
URL	https://masiso.pl/wp-login.php
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: wp-submit=Log In The user-controlled value was: log in
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?action=lostpassword appears to include user input in: a(n) [form] tag [id] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?action=lostpassword appears to include user input in: a(n) [form] tag [name] attribute The user input found was: action=lostpassword The user-controlled value was: lostpasswordform
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?action=lostpassword appears to include user input in: a(n) [input] tag [value] attribute The user input found was: action=lostpassword The user-controlled value was: lostpassword
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?action=lostpassword appears to include user input in: a(n) [input] tag [value] attribute The

	user input found was: user_login=ZAP The user-controlled value was: zap
URL	https://masiso.pl/wp-login.php?action=lostpassword
Metody	POST
Atak	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://masiso.pl/wp-login.php?action=lostpassword appears to include user input in: a(n) [input] tag [value] attribute The user input found was: wp-submit=Get New Password The user-controlled value was: get new password
Instances	78
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute
CWE Id	20
WASC Id	20
Plugin Id	10031