Email Server

Site: http://172.16.2.86

Generated on Tue, 5 Dec 2023 05:32:47

ZAP Version: 2.14.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	5
Informational	6

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	142
Content Security Policy (CSP) Header Not Set	Medium	102
Vulnerable JS Library	Medium	6
Big Redirect Detected (Potential Sensitive Information Leak)	Low	1
Cookie No HttpOnly Flag	Low	39
Cookie without SameSite Attribute	Low	42
Timestamp Disclosure - Unix	Low	168
X-Content-Type-Options Header Missing	Low	1
Authentication Request Identified	Informational	15
Cookie Poisoning	Informational	39
Information Disclosure - Suspicious Comments	Informational	174
Modern Web Application	Informational	58
Session Management Response Identified	Informational	6
User Controllable HTML Element Attribute (Potential XSS)	Informational	39

Alert Detail

Medium	Absence of Anti-CSRF Tokens
	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL /form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they

Description	can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://172.16.2.86
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=cs-cz
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">

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: "logout"].
URL	http://172.16.2.86/?lang=cs-cz
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=da-dk
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=da-dk
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=de-de
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=de-de
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=en-gb
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken,

Other Info	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: "logout"].
URL	http://172.16.2.86/?lang=en-gb
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=es-es
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=es-es
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=fi-fi
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=fi-fi
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=fr-fr
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
Other	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token,

Info	_csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "logout"].
URL	http://172.16.2.86/?lang=fr-fr
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=gr-gr
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=gr-gr
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=hu-hu
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=hu-hu
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=it-it
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=it-it
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=ko-kr
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=ko-kr
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=lv-lv
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=lv-lv
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=nl-nl
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].

URL	http://172.16.2.86/?lang=nl-nl
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=pl-pl
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=pl-pl
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=pt-br
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=pt-br
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=pt-pt
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].

URL	http://172.16.2.86/?lang=pt-pt
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=ro-ro
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=ro-ro
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=ru-ru
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=ru-ru
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=si-si
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=si-si

Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=sk-sk
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=sk-sk
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=sv-se
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=sv-se
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=tr-tr
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=tr-tr

Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=uk-ua
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=uk-ua
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=zh-cn
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=zh-cn
Method	GET
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=zh-tw
Method	GET
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=zh-tw
Method	GET

Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/SOGo/
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5"

	"3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%

URL	252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET

Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">

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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%

URL	2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">

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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET

Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/index/
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/index/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/index/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/SOGo/
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].

URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">

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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/
Method	POST
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=cs-cz
Method	POST
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=cs-cz
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=da-dk

Method	POST
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=da-dk
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=de-de
Method	POST
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=de-de
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=en-gb
Method	POST
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=en-gb
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=es-es
Method	POST

Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=es-es
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=fi-fi
Method	POST
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=fi-fi
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=fr-fr
Method	POST
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=fr-fr
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=gr-gr
Method	POST

Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=gr-gr
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=hu-hu
Method	POST
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=hu-hu
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=ko-kr
Method	POST
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=ko-kr
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=si-si
Method	POST
Attack	

Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=si-si
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=sk-sk
Method	POST
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=sk-sk
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=sv-se
Method	POST
Attack	
Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=sv-se
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/?lang=uk-ua
Method	POST
Attack	

Evidence	<form action="/" method="post" id="logout">
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: "logout"].
URL	http://172.16.2.86/?lang=uk-ua
Method	POST
Attack	
Evidence	<form method="post" autofill="off">
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: "login_user" "pass_user"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	

Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5"

	"3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	

Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/index/
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	<form method="post" ng-cloak="ng-cloak" ng-submit="app.login()" layout="column" name="loginForm">
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: "3.1.1.3.3.1.4.4.1.3.1.1.13.4.1.2.1.1.5" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.1.3" "3.1.1.3.3.1.4.4.1.3.1.1.13.7.9.1.3.3" "3.1.1.3.3.1.4.4.1.3.1.1.3.1.5" "newPasswordConfirmation" "passwordField"].
Instances	142

Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
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

Medium	**Content Security Policy (CSP) Header Not Set**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://172.16.2.86
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/
Method	GET
Attack	

Evidence	
Other Info	
URL	http://172.16.2.86/%5C%22https:%5C/%5C/upgrade.yubico.com%5C/getapikey%5C/%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=cs-cz
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=da-dk
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=de-de
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=en-gb
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=es-es
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=fi-fi
Method	GET
Attack	
Evidence	

Other Info	
URL	http://172.16.2.86/?lang=fr-fr
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=gr-gr
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=hu-hu
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=it-it
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=ko-kr
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=lv-lv
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=nl-nl
Method	GET
Attack	
Evidence	
Other Info	

URL	http://172.16.2.86/?lang=pl-pl
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=pt-br
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=pt-pt
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=ro-ro
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=ru-ru
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=si-si
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=sk-sk
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=sv-se
Method	GET

Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=tr-tr
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=uk-ua
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=zh-cn
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=zh-tw
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET

Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	

Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	

Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	

URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	

Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/index/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/index/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/index/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	

Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/SOGo/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET

Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=cs-cz
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=da-dk
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=de-de
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=en-gb
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=es-es
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=fi-fi
Method	POST
Attack	
Evidence	

Other Info	
URL	http://172.16.2.86/?lang=fr-fr
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=gr-gr
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=hu-hu
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=ko-kr
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=si-si
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=sk-sk
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/?lang=sv-se
Method	POST
Attack	
Evidence	
Other Info	

URL	http://172.16.2.86/?lang=uk-ua
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	

Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST

Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/index/
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	
Other Info	
Instances	102
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	Vulnerable JS Library
Description	The identified library angularjs, version 1.8.3 is vulnerable.
	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular-animate.min.js?

URL	lm=1695981119
Method	GET
Attack	
Evidence	/* AngularJS v1.8.3
Other Info	
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular-aria.min.js?lm=1695981119
Method	GET
Attack	
Evidence	/* AngularJS v1.8.3
Other Info	
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular-cookies.min.js?lm=1695981119
Method	GET
Attack	
Evidence	/* AngularJS v1.8.3
Other Info	
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular-messages.min.js?lm=1695981119
Method	GET
Attack	
Evidence	/* AngularJS v1.8.3
Other Info	
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular-sanitize.min.js?lm=1695981119
Method	GET
Attack	
Evidence	/* AngularJS v1.8.3
Other Info	
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular.min.js?lm=1695981119
Method	GET
Attack	
Evidence	/* AngularJS v1.8.3
Other Info	
Instances	6
Solution	Please upgrade to the latest version of angularjs.
Reference	https://blog.angular.io/discontinued-long-term-support-for-angularjs-cc066b82e65a?gi=9d3103b5445c
CWE Id	829

WASC Id	
Plugin Id	10003

Low	**Big Redirect Detected (Potential Sensitive Information Leak)**
Description	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://172.16.2.86/
Method	POST
Attack	
Evidence	
Other Info	Location header URI length: 1 [/]. Predicted response size: 301. Response Body Length: 25,884.
Instances	1
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

Low	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	http://172.16.2.86/?lang=cs-cz
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=da-dk
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=de-de
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=en-gb
Method	GET
Attack	

Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=es-es
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=fi-fi
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=fr-fr
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=gr-gr
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=hu-hu
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=it-it
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=ko-kr
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale

Other Info	
URL	http://172.16.2.86/?lang=lv-lv
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=nl-nl
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=pl-pl
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=pt-br
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=pt-pt
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=ro-ro
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=ru-ru
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	

URL	http://172.16.2.86/?lang=si-si
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=sk-sk
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=sv-se
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=tr-tr
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=uk-ua
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=zh-cn
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=zh-tw
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=cs-cz
Method	POST

Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=da-dk
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=de-de
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=en-gb
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=es-es
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=fi-fi
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=fr-fr
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=gr-gr
Method	POST
Attack	

Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=hu-hu
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=ko-kr
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=si-si
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=sk-sk
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=sv-se
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=uk-ua
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
Instances	39
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

Low	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	http://172.16.2.86
Method	GET
Attack	
Evidence	Set-Cookie: PHPSESSID
Other Info	
URL	http://172.16.2.86/
Method	GET
Attack	
Evidence	Set-Cookie: PHPSESSID
Other Info	
URL	http://172.16.2.86/?lang=cs-cz
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=da-dk
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=de-de
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=en-gb
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=es-es
Method	GET
Attack	

Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=fi-fi
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=fr-fr
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=gr-gr
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=hu-hu
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=it-it
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=ko-kr
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=lv-lv
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale

Other Info	
URL	http://172.16.2.86/?lang=nl-nl
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=pl-pl
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=pt-br
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=pt-pt
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=ro-ro
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=ru-ru
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=si-si
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	

URL	http://172.16.2.86/?lang=sk-sk
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=sv-se
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=tr-tr
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=uk-ua
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=zh-cn
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=zh-tw
Method	GET
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/
Method	POST
Attack	
Evidence	Set-Cookie: PHPSESSID
Other Info	
URL	http://172.16.2.86/?lang=cs-cz
Method	POST

Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=da-dk
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=de-de
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=en-gb
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=es-es
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=fi-fi
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=fr-fr
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=gr-gr
Method	POST
Attack	

Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=hu-hu
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=ko-kr
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=si-si
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=sk-sk
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=sv-se
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
URL	http://172.16.2.86/?lang=uk-ua
Method	POST
Attack	
Evidence	Set-Cookie: mailcow_locale
Other Info	
Instances	42
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

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server - Unix
URL	http://172.16.2.86
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=cs-cz
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=da-dk
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=de-de
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=en-gb
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=es-es
Method	GET
Attack	
Evidence	1701618688

Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=fi-fi
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=fr-fr
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=gr-gr
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=hu-hu
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=it-it
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=ko-kr
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=lv-lv
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28

URL	http://172.16.2.86/?lang=nl-nl
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=pl-pl
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=pt-br
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=pt-pt
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=ro-ro
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=ru-ru
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=si-si
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=sk-sk
Method	GET

Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=sv-se
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=tr-tr
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=uk-ua
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=zh-cn
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=zh-tw
Method	GET
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/cache/24933fadffd372bca5e61ec640d62bec947ad6f4.js
Method	GET
Attack	
Evidence	1518500249
Other Info	1518500249, which evaluates to: 2018-02-13 00:37:29
URL	http://172.16.2.86/cache/24933fadffd372bca5e61ec640d62bec947ad6f4.js
Method	GET
Attack	

Evidence	1732584193
Other Info	1732584193, which evaluates to: 2024-11-25 20:23:13
URL	http://172.16.2.86/cache/24933fadffd372bca5e61ec640d62bec947ad6f4.js
Method	GET
Attack	
Evidence	1859775393
Other Info	1859775393, which evaluates to: 2028-12-06 23:16:33
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/Common.js?lm=1695981119
Method	GET
Attack	
Evidence	1700485571
Other Info	1700485571, which evaluates to: 2023-11-20 08:06:11
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/Common.js?lm=1695981119
Method	GET
Attack	
Evidence	1732584193
Other Info	1732584193, which evaluates to: 2024-11-25 20:23:13
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/Common.js?lm=1695981119
Method	GET
Attack	
Evidence	1735328473
Other Info	1735328473, which evaluates to: 2024-12-27 14:41:13
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/Common.js?lm=1695981119
Method	GET
Attack	
Evidence	1770035416
Other Info	1770035416, which evaluates to: 2026-02-02 07:30:16
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/Common.js?lm=1695981119
Method	GET
Attack	
Evidence	1804603682
Other Info	1804603682, which evaluates to: 2027-03-09 09:48:02
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/Common.js?lm=1695981119
Method	GET
Attack	
Evidence	1839030562
Other	

Info	1839030562, which evaluates to: 2028-04-10 21:49:22
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/Common.js?lm=1695981119
Method	GET
Attack	
Evidence	1873313359
Other Info	1873313359, which evaluates to: 2029-05-12 16:49:19
URL	http://172.16.2.86/SOGo/
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET

Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET

Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	

Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	

Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565

Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25

URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119

Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.

	html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565

Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/index/
Method	GET
Attack	
Evidence	1695981119
Other	

Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/index/
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/index/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/index/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/index/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/index/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/SOGo/
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/SOGo/
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25

URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	

Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/
Method	POST
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=cs-cz
Method	POST
Attack	

Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=da-dk
Method	POST
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=de-de
Method	POST
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=en-gb
Method	POST
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=es-es
Method	POST
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=fi-fi
Method	POST
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=fr-fr
Method	POST
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=gr-gr
Method	POST
Attack	
Evidence	1701618688
Other	

Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=hu-hu
Method	POST
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=ko-kr
Method	POST
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=si-si
Method	POST
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=sk-sk
Method	POST
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=sv-se
Method	POST
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/?lang=uk-ua
Method	POST
Attack	
Evidence	1701618688
Other Info	1701618688, which evaluates to: 2023-12-03 10:51:28
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59

URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1701618565

Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22

Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other	

Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other	

Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/index/
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/index/
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1695981119
Other Info	1695981119, which evaluates to: 2023-09-29 05:51:59
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	1701618565
Other Info	1701618565, which evaluates to: 2023-12-03 10:49:25
Instances	168
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

Low	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://172.16.2.86/img/cow_mailcow.svg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for 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	1
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	Authentication Request Identified
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	http://172.16.2.86/
Method	POST
Attack	
Evidence	pass_user
Other Info	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.16.2.86/
URL	http://172.16.2.86/?lang=cs-cz
Method	POST
Attack	
Evidence	pass_user
Other Info	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.16.2.86/?lang=cs-cz
URL	http://172.16.2.86/?lang=da-dk
Method	POST
Attack	

Evidence	pass_user
Other Info	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.16.2.86/?lang=da-dk
URL	http://172.16.2.86/?lang=de-de
Method	POST
Attack	
Evidence	pass_user
Other Info	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.16.2.86/?lang=de-de
URL	http://172.16.2.86/?lang=en-gb
Method	POST
Attack	
Evidence	pass_user
Other Info	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.16.2.86/?lang=en-gb
URL	http://172.16.2.86/?lang=es-es
Method	POST
Attack	
Evidence	pass_user
Other Info	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.16.2.86/?lang=es-es
URL	http://172.16.2.86/?lang=fi-fi
Method	POST
Attack	
Evidence	pass_user
Other Info	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.16.2.86/?lang=fi-fi
URL	http://172.16.2.86/?lang=fr-fr
Method	POST
Attack	
Evidence	pass_user
Other Info	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.16.2.86/?lang=fr-fr
URL	http://172.16.2.86/?lang=gr-gr
Method	POST
Attack	
Evidence	pass_user
Other Info	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.16.2.86/?lang=gr-gr
URL	http://172.16.2.86/?lang=hu-hu
Method	POST
Attack	
Evidence	pass_user
Other	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.

Info	16.2.86/?lang=hu-hu
URL	http://172.16.2.86/?lang=ko-kr
Method	POST
Attack	
Evidence	pass_user
Other Info	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.16.2.86/?lang=ko-kr
URL	http://172.16.2.86/?lang=si-si
Method	POST
Attack	
Evidence	pass_user
Other Info	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.16.2.86/?lang=si-si
URL	http://172.16.2.86/?lang=sk-sk
Method	POST
Attack	
Evidence	pass_user
Other Info	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.16.2.86/?lang=sk-sk
URL	http://172.16.2.86/?lang=sv-se
Method	POST
Attack	
Evidence	pass_user
Other Info	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.16.2.86/?lang=sv-se
URL	http://172.16.2.86/?lang=uk-ua
Method	POST
Attack	
Evidence	pass_user
Other Info	userParam=login_user userValue=ZAP passwordParam=pass_user referer=http://172.16.2.86/?lang=uk-ua
Instances	15
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/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	**Cookie Poisoning**
Description	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	http://172.16.2.86/?lang=cs-cz
Method	GET

Attack	
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: http://172.16.2.86/?lang=cs-cz User-input was found in the following cookie: mailcow_locale=cs-cz; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=cs-cz
URL	http://172.16.2.86/?lang=da-dk
Method	GET
Attack	
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: http://172.16.2.86/?lang=da-dk User-input was found in the following cookie: mailcow_locale=da-dk; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=da-dk
URL	http://172.16.2.86/?lang=de-de
Method	GET
Attack	
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: http://172.16.2.86/?lang=de-de User-input was found in the following cookie: mailcow_locale=de-de; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=de-de
URL	http://172.16.2.86/?lang=en-gb
Method	GET
Attack	
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: http://172.16.2.86/?lang=en-gb User-input was found in the following cookie: mailcow_locale=en-gb; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=en-gb
URL	http://172.16.2.86/?lang=es-es
Method	GET
Attack	
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: http://172.16.2.86/?lang=es-es User-input was found in the following cookie: mailcow_locale=es-es; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=es-es
URL	http://172.16.2.86/?lang=fi-fi
Method	GET
Attack	
Evidence	
Other	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: http://172.16.2.86/?lang=fi-fi User-input was

Info	found in the following cookie: mailcow_locale=fi-fi; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=fi-fi
URL	http://172.16.2.86/?lang=fr-fr
Method	GET
Attack	
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: http://172.16.2.86/?lang=fr-fr User-input was found in the following cookie: mailcow_locale=fr-fr; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=fr-fr
URL	http://172.16.2.86/?lang=gr-gr
Method	GET
Attack	
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: http://172.16.2.86/?lang=gr-gr User-input was found in the following cookie: mailcow_locale=gr-gr; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=gr-gr
URL	http://172.16.2.86/?lang=hu-hu
Method	GET
Attack	
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: http://172.16.2.86/?lang=hu-hu User-input was found in the following cookie: mailcow_locale=hu-hu; expires=Mon, 25 Nov 2024 10:24: 29 GMT; Max-Age=30758400 The user input was: lang=hu-hu
URL	http://172.16.2.86/?lang=it-it
Method	GET
Attack	
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: http://172.16.2.86/?lang=it-it User-input was found in the following cookie: mailcow_locale=it-it; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=it-it
URL	http://172.16.2.86/?lang=ko-kr
Method	GET
Attack	
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: http://172.16.2.86/?lang=ko-kr User-input was found in the following cookie: mailcow_locale=ko-kr; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=ko-kr
URL	http://172.16.2.86/?lang=lv-lv
Method	GET
Attack	

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: http://172.16.2.86/?lang=lv-lv User-input was found in the following cookie: mailcow_locale=lv-lv; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=lv-lv
URL	http://172.16.2.86/?lang=nl-nl
Method	GET
Attack	
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: http://172.16.2.86/?lang=nl-nl User-input was found in the following cookie: mailcow_locale=nl-nl; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=nl-nl
URL	http://172.16.2.86/?lang=pl-pl
Method	GET
Attack	
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: http://172.16.2.86/?lang=pl-pl User-input was found in the following cookie: mailcow_locale=pl-pl; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=pl-pl
URL	http://172.16.2.86/?lang=pt-br
Method	GET
Attack	
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: http://172.16.2.86/?lang=pt-br User-input was found in the following cookie: mailcow_locale=pt-br; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=pt-br
URL	http://172.16.2.86/?lang=pt-pt
Method	GET
Attack	
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: http://172.16.2.86/?lang=pt-pt User-input was found in the following cookie: mailcow_locale=pt-pt; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=pt-pt
URL	http://172.16.2.86/?lang=ro-ro
Method	GET
Attack	
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: http://172.16.2.86/?lang=ro-ro User-input was found in the following cookie: mailcow_locale=ro-ro; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=ro-ro

URL	http://172.16.2.86/?lang=ru-ru
Method	GET
Attack	
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: http://172.16.2.86/?lang=ru-ru User-input was found in the following cookie: mailcow_locale=ru-ru; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=ru-ru
URL	http://172.16.2.86/?lang=si-si
Method	GET
Attack	
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: http://172.16.2.86/?lang=si-si User-input was found in the following cookie: mailcow_locale=si-si; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=si-si
URL	http://172.16.2.86/?lang=sk-sk
Method	GET
Attack	
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: http://172.16.2.86/?lang=sk-sk User-input was found in the following cookie: mailcow_locale=sk-sk; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=sk-sk
URL	http://172.16.2.86/?lang=sv-se
Method	GET
Attack	
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: http://172.16.2.86/?lang=sv-se User-input was found in the following cookie: mailcow_locale=sv-se; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=sv-se
URL	http://172.16.2.86/?lang=tr-tr
Method	GET
Attack	
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: http://172.16.2.86/?lang=tr-tr User-input was found in the following cookie: mailcow_locale=tr-tr; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=tr-tr
URL	http://172.16.2.86/?lang=uk-ua
Method	GET
Attack	
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: http://172.16.2.86/?lang=uk-ua User-input was found in the following cookie: mailcow_locale=uk-ua; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=uk-ua
URL	http://172.16.2.86/?lang=zh-cn
Method	GET
Attack	
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: http://172.16.2.86/?lang=zh-cn User-input was found in the following cookie: mailcow_locale=zh-cn; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=zh-cn
URL	http://172.16.2.86/?lang=zh-tw
Method	GET
Attack	
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: http://172.16.2.86/?lang=zh-tw User-input was found in the following cookie: mailcow_locale=zh-tw; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=zh-tw
URL	http://172.16.2.86/?lang=cs-cz
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: http://nottrusted.com/page?value=maliciousInput. This was identified at: http://172.16.2.86/?lang=cs-cz User-input was found in the following cookie: mailcow_locale=cs-cz; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=cs-cz
URL	http://172.16.2.86/?lang=da-dk
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: http://nottrusted.com/page?value=maliciousInput. This was identified at: http://172.16.2.86/?lang=da-dk User-input was found in the following cookie: mailcow_locale=da-dk; expires=Mon, 25 Nov 2024 10:24:41 GMT; Max-Age=30758400 The user input was: lang=da-dk
URL	http://172.16.2.86/?lang=de-de
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: http://nottrusted.com/page?

	value=maliciousInput. This was identified at: http://172.16.2.86/?lang=de-de User-input was found in the following cookie: mailcow_locale=de-de; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=de-de
URL	http://172.16.2.86/?lang=en-gb
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: http://nottrusted.com/page?value=maliciousInput. This was identified at: http://172.16.2.86/?lang=en-gb User-input was found in the following cookie: mailcow_locale=en-gb; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=en-gb
URL	http://172.16.2.86/?lang=es-es
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: http://nottrusted.com/page?value=maliciousInput. This was identified at: http://172.16.2.86/?lang=es-es User-input was found in the following cookie: mailcow_locale=es-es; expires=Mon, 25 Nov 2024 10:24:29 GMT; Max-Age=30758400 The user input was: lang=es-es
URL	http://172.16.2.86/?lang=fi-fi
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: http://nottrusted.com/page?value=maliciousInput. This was identified at: http://172.16.2.86/?lang=fi-fi User-input was found in the following cookie: mailcow_locale=fi-fi; expires=Mon, 25 Nov 2024 10:24:35 GMT; Max-Age=30758400 The user input was: lang=fi-fi
URL	http://172.16.2.86/?lang=fr-fr
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: http://nottrusted.com/page?value=maliciousInput. This was identified at: http://172.16.2.86/?lang=fr-fr User-input was found in the following cookie: mailcow_locale=fr-fr; expires=Mon, 25 Nov 2024 10:24:30 GMT; Max-Age=30758400 The user input was: lang=fr-fr
URL	http://172.16.2.86/?lang=gr-gr
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: http://nottrusted.com/page?

	value=maliciousInput. This was identified at: http://172.16.2.86/?lang=gr-gr User-input was found in the following cookie: mailcow_locale=gr-gr; expires=Mon, 25 Nov 2024 10:24:38 GMT; Max-Age=30758400 The user input was: lang=gr-gr
URL	http://172.16.2.86/?lang=hu-hu
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: http://nottrusted.com/page?value=maliciousInput. This was identified at: http://172.16.2.86/?lang=hu-hu User-input was found in the following cookie: mailcow_locale=hu-hu; expires=Mon, 25 Nov 2024 10:24:31 GMT; Max-Age=30758400 The user input was: lang=hu-hu
URL	http://172.16.2.86/?lang=ko-kr
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: http://nottrusted.com/page?value=maliciousInput. This was identified at: http://172.16.2.86/?lang=ko-kr User-input was found in the following cookie: mailcow_locale=ko-kr; expires=Mon, 25 Nov 2024 10:24:33 GMT; Max-Age=30758400 The user input was: lang=ko-kr
URL	http://172.16.2.86/?lang=si-si
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: http://nottrusted.com/page?value=maliciousInput. This was identified at: http://172.16.2.86/?lang=si-si User-input was found in the following cookie: mailcow_locale=si-si; expires=Mon, 25 Nov 2024 10:25:34 GMT; Max-Age=30758400 The user input was: lang=si-si
URL	http://172.16.2.86/?lang=sk-sk
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: http://nottrusted.com/page?value=maliciousInput. This was identified at: http://172.16.2.86/?lang=sk-sk User-input was found in the following cookie: mailcow_locale=sk-sk; expires=Mon, 25 Nov 2024 10:25:42 GMT; Max-Age=30758400 The user input was: lang=sk-sk
URL	http://172.16.2.86/?lang=sv-se
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: http://nottrusted.com/page?

	value=maliciousInput. This was identified at: http://172.16.2.86/?lang=sv-se User-input was found in the following cookie: mailcow_locale=sv-se; expires=Mon, 25 Nov 2024 10:25:51 GMT; Max-Age=30758400 The user input was: lang=sv-se
URL	http://172.16.2.86/?lang=uk-ua
Method	POST
Attack	
Evidence	
Other Info	An attacker may be able to poison cookie values through POST parameters. To test if this is a more serious issue, you should try resending that request as a GET, with the POST parameter included as a query string parameter. For example: http://nottrusted.com/page?value=maliciousInput. This was identified at: http://172.16.2.86/?lang=uk-ua User-input was found in the following cookie: mailcow_locale=uk-ua; expires=Mon, 25 Nov 2024 10:26:20 GMT; Max-Age=30758400 The user input was: lang=uk-ua
Instances	39
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	20
WASC Id	20
Plugin Id	10029

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	http://172.16.2.86
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion"," delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion"," delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=cs-cz
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Zru\u0161it","confirm_delete":"Potvdit smaz\u00e1n\u00ed","delete_now":"Smazat","delete_", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=da-dk

Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Afbestille","confirm_delete":"Bekr\u00e6ft sletning","delete_now":"Slet nu","delete_thes", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=de-de
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Abbrechen","confirm_delete":"L\u00f6schen best\u00e4tigen","delete_now":"Jetzt l\u00f6sc", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=en-gb
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion","delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=es-es
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion","delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=fi-fi
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Peruuta","confirm_delete":"Poiston vahvistaminen","delete_now":"Poista nyt","delete_thes", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/?lang=fr-fr
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Annuler","confirm_delete":"Confirmer la suppression","delete_now":"Effacer maintenant","", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=gr-gr
Method	GET
Attack	

Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion"," delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=hu-hu
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"M\u00e9gse","confirm_delete":"T\u00f6rl\u00e9s meger\u0151s\u00edt\u00e9se","delete_now"", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=it-it
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Annulla","confirm_delete":"Conferma eliminazione"," delete_now":"Elimina ora","delete_the", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/?lang=ko-kr
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion"," delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=lv-lv
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Atcelt","confirm_delete":"Apstiprin\u0101t dz\u0113\u0161anu","delete_now":"Dz\u0113st t", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=nl-nl
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Annuleren","confirm_delete":"Bevestig verwijdering"," delete_now":"Nu verwijderen","delet", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/?lang=pl-pl
Method	GET
Attack	

Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Anuluj","confirm_delete":"Potwierd\u017a usuni\u0119cie","delete_now":"Usu\u0144 teraz",", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=pt-br
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancelar","confirm_delete":"Confirme a exclus\u00e3o","delete_now":"Excluir agora","dele", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=pt-pt
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion"," delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=ro-ro
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Anuleaz\u0103","confirm_delete":"Confirm\u0103 \u0219tergerea","delete_now":"\u0218terge", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/?lang=ru-ru
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"\u041e\u0442\u043c\u0435\u043d\u0430","confirm_delete":"\u041f\u043e\u0434\u0442\u0432\u0435\u", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=si-si
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion"," delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=sk-sk
Method	GET
Attack	
Evidence	select

Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Zru\u0161i\u0165","confirm_delete":"Potvr\u010fte vymazanie","delete_now":"Vymaza\u0165 ", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/?lang=sv-se
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Avbryt","confirm_delete":"Bekr\u00e4fta borttagning","delete_now":"Ta bort nu","delete_t", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=tr-tr
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion","delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=uk-ua
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"\u0421\u043a\u0430\u0441\u0443\u0432\u0430\u0442\u0438","confirm_delete":"\u041f\u0456\u", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=zh-cn
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"\u53d6\u6d88","confirm_delete":"\u786e\u8ba4\u5220\u9664","delete_now":"\u7acb\u5373\u52", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=zh-tw
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"\u53d6\u6d88","confirm_delete":"\u78ba\u8a8d\u522a\u9664","delete_now":"\u7acb\u5373\u52", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/cache/24933fadffd372bca5e61ec640d62bec947ad6f4.js
Method	GET
Attack	
Evidence	from
	The following pattern was used: \bFROM\b and was detected 18 times, the first in the

Other Info	element starting with: "return resolved.replace('%d',plural)});DataTable.version="1.13.1"; DataTable.settings=[];DataTable.models={};DataTable.models.oSe", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/cache/24933fadffd372bca5e61ec640d62bec947ad6f4.js
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 65 times, the first in the element starting with: "!function(t,e){"object"==typeof exports&&"undefined"!=typeof module? module.exports=e():"function"==typeof define&&define.amd?def", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/cache/24933fadffd372bca5e61ec640d62bec947ad6f4.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 7 times, the first in the element starting with: "oInit=_fnExtend($.extend(!0,{},defaults),oInit);_fnMap(oSettings. oFeatures,oInit,["bPaginate","bLengthChange","bFilter","bSort",", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/cache/24933fadffd372bca5e61ec640d62bec947ad6f4.js
Method	GET
Attack	
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	http://172.16.2.86/cache/24933fadffd372bca5e61ec640d62bec947ad6f4.js
Method	GET
Attack	
Evidence	xxx
Other Info	The following pattern was used: \bXXX\b and was detected in the element starting with: "! function(e,r){"object"==typeof exports&&"undefined"!=typeof module?module.exports=r():" function"==typeof define&&define.amd?def", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/Common.js?lm=1695981119
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "function l(){var n,e,t=arguments[0],o=t,r=arguments;for(labels[t]?o=labels[t]:clabels[t]&& (o=clabels[t]),n=1,e=0;n<r.length;n++,", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/Main.js?lm=1695981119
Method	GET
Attack	
Evidence	user
Other	The following pattern was used: \bUSER\b and was detected in the element starting with: "! function(){"use strict";angular.module("SOGo.MainUI",["SOGo.Common","SOGo.

Info	Authentication"]);function e(e,o,s,r,a,n,i,t){var d=t", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular-animate.min.js?lm=1695981119
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 14 times, the first in the element starting with: "(function(Y,z){'use strict';function Fa(a,b,c){if(!a)throw Pa("areq", b||"?",c||"required");return a}function Ga(a,b){if(!a&&!b)r", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular-aria.min.js?lm=1695981119
Method	GET
Attack	
Evidence	SELECT
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "(function(t,l){'use strict';var c="BUTTON A INPUT TEXTAREA SELECT DETAILS SUMMARY".split(" "),m=function(a,e){if(-1!==e.indexOf(", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular-material.min.js?lm=1695981119
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "!function(L,be,ge){"use strict";function e(e,t){if(t.has("$swipe")){e.warn("You are using the ngTouch module. \nAngularJS Materi", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular-sanitize.min.js?lm=1695981119
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "p=h("accent-height,accumulate,additive,alphabetic,arabic-form,ascent,baseProfile,bbox, begin,by,calcMode,cap-height,class,color,c", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular-ui-router.min.js?lm=1695981119
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "!function(t,e){"object"==typeof exports&&"undefined"!=typeof module?e(exports,require ("angular")):"function"==typeof define&&def", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular.min.js?lm=1695981119
Method	GET
Attack	

Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected 9 times, the first in the element starting with: "b[c]))return!1;return!0}}else{if(ha(a))return ha(b)?ec(a.getTime(),b.getTime()):!1;if(ab(a))return ab(b)?a.toString()===b.toStri", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular.min.js?lm=1695981119
Method	GET
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected 2 times, the first in the element starting with: "(a=a.message+"\n"+a.sourceURL+":"+a.line));return a}function e(a){var b=d.console||{},e=b[a]||b.log||E;return function(){var a=[", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular.min.js?lm=1695981119
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 3 times, the first in the element starting with: "k,h,l){l&&l();h=h||{};h.from&&g.css(h.from);h.to&&g.css(h.to);if(h.addClass||h.removeClass)if(k=h.addClass,l=h.removeClass,h=a.g", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo.woa/WebServerResources/js/vendor/angular.min.js?lm=1695981119
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 7 times, the first in the element starting with: "lc=Me(z);lc("ng",["ngLocale"],["$provide",function(a){a.provider({$$sanitizeUri:Qe});a.provider("$compile",Zc).directive({a:Re,i", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/'; var ResourcesURL = '/SOGo.woa/WebServ", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22

Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later

Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%

URL	252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	

Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.

URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET

Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment

	/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
	The following pattern was used: \bADMINISTRATOR\b and was detected in the element

Other Info	starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator

Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET

Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET

Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/index/
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/'; var ResourcesURL = '/SOGo.woa/WebServ", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/index/
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/index/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator

Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/index/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/index/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/index/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/SOGo/
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/'; var ResourcesURL = '/SOGo.woa/WebServ", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/SOGo/
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator
	The following pattern was used: \bADMINISTRATOR\b and was detected in the element

Other Info	starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator

Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/
Method	POST
Attack	
Evidence	admin
	The following pattern was used: \bADMIN\b and was detected in the element starting with:

Other Info	"<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion"," delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=cs-cz
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Zru\u0161it","confirm_delete":"Potvdit smaz\u00e1n\u00ed","delete_now":"Smazat","delete_", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=da-dk
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Afbestille","confirm_delete":"Bekr\u00e6ft sletning"," delete_now":"Slet nu","delete_thes", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=de-de
Method	POST
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Abbrechen","confirm_delete":"L\u00f6schen best\u00e4tigen","delete_now":"Jetzt l\u00f6sc", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=en-gb
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion"," delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=es-es
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion"," delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=fi-fi
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Peruuta","confirm_delete":"Poiston vahvistaminen"," delete_now":"Poista nyt","delete_thes", see evidence field for the suspicious comment

	/snippet.
URL	http://172.16.2.86/?lang=fr-fr
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Annuler","confirm_delete":"Confirmer la suppression"," delete_now":"Effacer maintenant","", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=gr-gr
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion"," delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=hu-hu
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"M\u00e9gse","confirm_delete":"T\u00f6rl\u00e9s meger\u0151s\u00edt\u00e9se","delete_now"", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=ko-kr
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion"," delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=si-si
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Cancel","confirm_delete":"Confirm deletion"," delete_now":"Delete now","delete_these_item", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=sk-sk
Method	POST
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Zru\u0161i\u0165","confirm_delete":"Potvr\u010fte vymazanie","delete_now":"Vymaza\u0165 ", see evidence field for the suspicious comment /snippet.

URL	http://172.16.2.86/?lang=sv-se
Method	POST
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":"Avbryt","confirm_delete":"Bekr\u00e4fta borttagning"," delete_now":"Ta bort nu","delete_t", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/?lang=uk-ua
Method	POST
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "<script> var lang_footer = {"cancel":" \u0421\u043a\u0430\u0441\u0443\u0432\u0430\u0442\u0438","confirm_delete":" \u041f\u0456\u", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.

URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	later
Other	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100">

Info	<md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	

Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST

Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	

Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/index/
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/'; var ResourcesURL = '/SOGo.woa/WebServ", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/index/
Method	POST
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	administrator
Other Info	The following pattern was used: \bADMINISTRATOR\b and was detected in the element starting with: "<script type="text/javascript"> var ApplicationBaseURL = '/SOGo/so/'; var ResourcesURL = '/SOGo.woa/WebS", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	later

Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "<script id="aboutBox.html" type="text/ng-template"> <md-dialog flex="50" flex-xs="100"> <md-dialog-content class="md-d", see evidence field for the suspicious comment/snippet.
Instances	174
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

Informational	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://172.16.2.86/SOGo/
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22

Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/gnu.org/licenses/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other	Links have been found that do not have traditional href attributes, which is an indication that

Info	this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	

Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%2525255C%25252522http:/www.sogo.nu/en/support/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	

Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	

Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/index/
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/index/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/index/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.

URL	http://172.16.2.86/SOGo/SOGo/
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	GET
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	GET

Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/gnu.org/licenses/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	

Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%25255C%252522http:/www.sogo.nu/en/support/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%255C%2522http:/gnu.org/licenses/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%255C%2522http:/www.sogo.nu/en/support/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	

Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/index/
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/gnu.org/licenses/gpl.html%5C%22
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://172.16.2.86/SOGo/SOGo/%5C%22http:/www.sogo.nu/en/support/community.html%5C%22
Method	POST
Attack	
Evidence	Password lost
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Instances	58
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Session Management Response Identified**

Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	http://172.16.2.86
Method	GET
Attack	
Evidence	6f55171247eb6411f66008b4a205b0f3
Other Info	cookie:PHPSESSID
URL	http://172.16.2.86
Method	GET
Attack	
Evidence	d01d885cb821d4da2f53182f059c7ab5
Other Info	cookie:PHPSESSID
URL	http://172.16.2.86/
Method	GET
Attack	
Evidence	7b3c02ee43b4a77a100982c5c0e3a8a2
Other Info	cookie:PHPSESSID
URL	http://172.16.2.86/
Method	POST
Attack	
Evidence	32bcd71b98bfdb3c330f6f317bab8333
Other Info	cookie:PHPSESSID
URL	http://172.16.2.86/
Method	GET
Attack	
Evidence	7b3c02ee43b4a77a100982c5c0e3a8a2
Other Info	cookie:PHPSESSID
URL	http://172.16.2.86/
Method	POST
Attack	
Evidence	32bcd71b98bfdb3c330f6f317bab8333
Other Info	cookie:PHPSESSID
Instances	6
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

Informational	User Controllable HTML Element Attribute (Potential XSS)
Description	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	http://172.16.2.86/?lang=cs-cz
Method	GET
Attack	
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: http://172.16.2.86/?lang=cs-cz appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=cs-cz The user-controlled value was: cs-cz
URL	http://172.16.2.86/?lang=da-dk
Method	GET
Attack	
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: http://172.16.2.86/?lang=da-dk appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=da-dk The user-controlled value was: da-dk
URL	http://172.16.2.86/?lang=de-de
Method	GET
Attack	
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: http://172.16.2.86/?lang=de-de appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=de-de The user-controlled value was: de-de
URL	http://172.16.2.86/?lang=en-gb
Method	GET
Attack	
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: http://172.16.2.86/?lang=en-gb appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=en-gb The user-controlled value was: en-gb
URL	http://172.16.2.86/?lang=es-es
Method	GET
Attack	
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: http://172.16.2.86/?lang=es-es appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=es-es The user-controlled value was: es-es
URL	http://172.16.2.86/?lang=fi-fi

Method	GET
Attack	
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: http://172.16.2.86/?lang=fi-fi appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=fi-fi The user-controlled value was: fi-fi
URL	http://172.16.2.86/?lang=fr-fr
Method	GET
Attack	
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: http://172.16.2.86/?lang=fr-fr appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=fr-fr The user-controlled value was: fr-fr
URL	http://172.16.2.86/?lang=gr-gr
Method	GET
Attack	
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: http://172.16.2.86/?lang=gr-gr appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=gr-gr The user-controlled value was: gr-gr
URL	http://172.16.2.86/?lang=hu-hu
Method	GET
Attack	
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: http://172.16.2.86/?lang=hu-hu appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=hu-hu The user-controlled value was: hu-hu
URL	http://172.16.2.86/?lang=it-it
Method	GET
Attack	
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: http://172.16.2.86/?lang=it-it appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=it-it The user-controlled value was: it-it
URL	http://172.16.2.86/?lang=ko-kr
Method	GET
Attack	
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: http://172.16.2.86/?lang=ko-kr appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=ko-kr The user-controlled value was: ko-kr
URL	http://172.16.2.86/?lang=lv-lv
Method	GET

Attack	
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: http://172.16.2.86/?lang=lv-lv appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=lv-lv The user-controlled value was: lv-lv
URL	http://172.16.2.86/?lang=nl-nl
Method	GET
Attack	
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: http://172.16.2.86/?lang=nl-nl appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=nl-nl The user-controlled value was: nl-nl
URL	http://172.16.2.86/?lang=pl-pl
Method	GET
Attack	
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: http://172.16.2.86/?lang=pl-pl appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=pl-pl The user-controlled value was: pl-pl
URL	http://172.16.2.86/?lang=pt-br
Method	GET
Attack	
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: http://172.16.2.86/?lang=pt-br appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=pt-br The user-controlled value was: pt-br
URL	http://172.16.2.86/?lang=pt-pt
Method	GET
Attack	
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: http://172.16.2.86/?lang=pt-pt appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=pt-pt The user-controlled value was: pt-pt
URL	http://172.16.2.86/?lang=ro-ro
Method	GET
Attack	
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: http://172.16.2.86/?lang=ro-ro appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=ro-ro The user-controlled value was: ro-ro
URL	http://172.16.2.86/?lang=ru-ru
Method	GET

Attack	
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: http://172.16.2.86/?lang=ru-ru appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=ru-ru The user-controlled value was: ru-ru
URL	http://172.16.2.86/?lang=si-si
Method	GET
Attack	
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: http://172.16.2.86/?lang=si-si appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=si-si The user-controlled value was: si-si
URL	http://172.16.2.86/?lang=sk-sk
Method	GET
Attack	
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: http://172.16.2.86/?lang=sk-sk appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=sk-sk The user-controlled value was: sk-sk
URL	http://172.16.2.86/?lang=sv-se
Method	GET
Attack	
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: http://172.16.2.86/?lang=sv-se appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=sv-se The user-controlled value was: sv-se
URL	http://172.16.2.86/?lang=tr-tr
Method	GET
Attack	
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: http://172.16.2.86/?lang=tr-tr appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=tr-tr The user-controlled value was: tr-tr
URL	http://172.16.2.86/?lang=uk-ua
Method	GET
Attack	
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: http://172.16.2.86/?lang=uk-ua appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=uk-ua The user-controlled value was: uk-ua
URL	http://172.16.2.86/?lang=zh-cn
Method	GET
Attack	

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: http://172.16.2.86/?lang=zh-cn appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=zh-cn The user-controlled value was: zh-cn
URL	http://172.16.2.86/?lang=zh-tw
Method	GET
Attack	
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: http://172.16.2.86/?lang=zh-tw appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=zh-tw The user-controlled value was: zh-tw
URL	http://172.16.2.86/?lang=cs-cz
Method	POST
Attack	
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: http://172.16.2.86/?lang=cs-cz appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=cs-cz The user-controlled value was: cs-cz
URL	http://172.16.2.86/?lang=da-dk
Method	POST
Attack	
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: http://172.16.2.86/?lang=da-dk appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=da-dk The user-controlled value was: da-dk
URL	http://172.16.2.86/?lang=de-de
Method	POST
Attack	
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: http://172.16.2.86/?lang=de-de appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=de-de The user-controlled value was: de-de
URL	http://172.16.2.86/?lang=en-gb
Method	POST
Attack	
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: http://172.16.2.86/?lang=en-gb appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=en-gb The user-controlled value was: en-gb
URL	http://172.16.2.86/?lang=es-es
Method	POST
Attack	

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: http://172.16.2.86/?lang=es-es appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=es-es The user-controlled value was: es-es
URL	http://172.16.2.86/?lang=fi-fi
Method	POST
Attack	
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: http://172.16.2.86/?lang=fi-fi appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=fi-fi The user-controlled value was: fi-fi
URL	http://172.16.2.86/?lang=fr-fr
Method	POST
Attack	
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: http://172.16.2.86/?lang=fr-fr appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=fr-fr The user-controlled value was: fr-fr
URL	http://172.16.2.86/?lang=gr-gr
Method	POST
Attack	
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: http://172.16.2.86/?lang=gr-gr appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=gr-gr The user-controlled value was: gr-gr
URL	http://172.16.2.86/?lang=hu-hu
Method	POST
Attack	
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: http://172.16.2.86/?lang=hu-hu appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=hu-hu The user-controlled value was: hu-hu
URL	http://172.16.2.86/?lang=ko-kr
Method	POST
Attack	
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: http://172.16.2.86/?lang=ko-kr appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=ko-kr The user-controlled value was: ko-kr
URL	http://172.16.2.86/?lang=si-si
Method	POST
Attack	
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: http://172.16.2.86/?lang=si-si appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=si-si The user-controlled value was: si-si
URL	http://172.16.2.86/?lang=sk-sk
Method	POST
Attack	
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: http://172.16.2.86/?lang=sk-sk appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=sk-sk The user-controlled value was: sk-sk
URL	http://172.16.2.86/?lang=sv-se
Method	POST
Attack	
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: http://172.16.2.86/?lang=sv-se appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=sv-se The user-controlled value was: sv-se
URL	http://172.16.2.86/?lang=uk-ua
Method	POST
Attack	
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: http://172.16.2.86/?lang=uk-ua appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: lang=uk-ua The user-controlled value was: uk-ua
Instances	39
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