Odoo Scan

Site: http://172.16.2.34:8069

Generated on Tue, 5 Dec 2023 14:11:37

ZAP Version: 2.14.0

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances
.htaccess Information Leak	Medium	4
Absence of Anti-CSRF Tokens	Medium	42
Content Security Policy (CSP) Header Not Set	Medium	15
Cross-Domain Misconfiguration	Medium	1
Missing Anti-clickjacking Header	Medium	7
Vulnerable JS Library	Medium	1
Cookie without SameSite Attribute	Low	21
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	43
X-Content-Type-Options Header Missing	Low	34
Authentication Request Identified	Informational	2
Information Disclosure - Suspicious Comments	Informational	28
Session Management Response Identified	Informational	24
User Agent Fuzzer	Informational	108
User Controllable HTML Element Attribute (Potential XSS)	Informational	14

Alert Detail

Medium	.htaccess Information Leak
Description	htaccess files can be used to alter the configuration of the Apache Web Server software to enable/disable additional functionality and features that the Apache Web Server software has to offer.
URL	http://172.16.2.34:8069/web/assets/199-59bbeaa/.htaccess
Method	GET
Attack	

Evidence	HTTP/1.0 200 OK
Other Info	
URL	http://172.16.2.34:8069/web/assets/204-cc89601/.htaccess
Method	GET
Attack	
Evidence	HTTP/1.0 200 OK
Other Info	
URL	http://172.16.2.34:8069/web/assets/205-9760593/.htaccess
Method	GET
Attack	
Evidence	HTTP/1.0 200 OK
Other Info	
URL	http://172.16.2.34:8069/web/assets/206-1ab8328/.htaccess
Method	GET
Attack	
Evidence	HTTP/1.0 200 OK
Other Info	
Instances	4
Solution	Ensure the .htaccess file is not accessible.
Reference	http://www.htaccess-guide.com/
CWE Id	94
WASC Id	14
Plugin Id	40032

Medium	**Absence of Anti-CSRF Tokens**
Description	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 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://172.16.2.34:8069/web/database/manager
Method	GET
Attack	
Evidence	<form role="form" action="/web/database/create" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "dbname" "load_demo_checkbox" "login" "master_pwd" "password" "phone"].
URL	http://172.16.2.34:8069/web/database/manager
Method	GET
Attack	
Evidence	<form id="form_restore_db" role="form" action="/web/database/restore" method="post" enctype="multipart/form-data">
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: "backup_file" "dbname_restore" "master_pwd" "radio_copy_false" "radio_copy_true"].
URL	http://172.16.2.34:8069/web/database/manager
Method	GET
Attack	
Evidence	<form id="form_change_pwd" role="form" action="/web/database/change_password" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 3: "master_pwd" "master_pwd_new"].
URL	http://172.16.2.34:8069/web/database/manager
Method	GET
Attack	
Evidence	<form id="form-duplicate-db" role="form" action="/web/database/duplicate" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 4: "dbname_duplicate" "master_pwd" "new_name"].
URL	http://172.16.2.34:8069/web/database/manager
Method	GET
Attack	
Evidence	<form id="form_drop_db" role="form" action="/web/database/drop" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 5: "dbname_delete" "master_pwd"].
URL	http://172.16.2.34:8069/web/database/manager
Method	GET
Attack	

Evidence	<form id="form_backup_db" role="form" action="/web/database/backup" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 6: "dbname_backup" "master_pwd"].
URL	http://172.16.2.34:8069/web/database/backup
Method	POST
Attack	
Evidence	<form role="form" action="/web/database/create" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "dbname" "load_demo_checkbox" "login" "master_pwd" "password" "phone"].
URL	http://172.16.2.34:8069/web/database/backup
Method	POST
Attack	
Evidence	<form id="form_restore_db" role="form" action="/web/database/restore" method="post" enctype="multipart/form-data">
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: "backup_file" "dbname_restore" "master_pwd" "radio_copy_false" "radio_copy_true"].
URL	http://172.16.2.34:8069/web/database/backup
Method	POST
Attack	
Evidence	<form id="form_change_pwd" role="form" action="/web/database/change_password" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 3: "master_pwd" "master_pwd_new"].
URL	http://172.16.2.34:8069/web/database/backup
Method	POST
Attack	
Evidence	<form id="form-duplicate-db" role="form" action="/web/database/duplicate" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 4: "dbname_duplicate" "master_pwd" "new_name"].
URL	http://172.16.2.34:8069/web/database/backup
Method	POST
Attack	
Evidence	<form id="form_drop_db" role="form" action="/web/database/drop" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 5: "dbname_delete" "master_pwd"].
URL	http://172.16.2.34:8069/web/database/backup

Method	POST
Attack	
Evidence	<form id="form_backup_db" role="form" action="/web/database/backup" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 6: "dbname_backup" "master_pwd"].
URL	http://172.16.2.34:8069/web/database/change_password
Method	POST
Attack	
Evidence	<form role="form" action="/web/database/create" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "dbname" "load_demo_checkbox" "login" "master_pwd" "password" "phone"].
URL	http://172.16.2.34:8069/web/database/change_password
Method	POST
Attack	
Evidence	<form id="form_restore_db" role="form" action="/web/database/restore" method="post" enctype="multipart/form-data">
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: "backup_file" "dbname_restore" "master_pwd" "radio_copy_false" "radio_copy_true"].
URL	http://172.16.2.34:8069/web/database/change_password
Method	POST
Attack	
Evidence	<form id="form_change_pwd" role="form" action="/web/database/change_password" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 3: "master_pwd" "master_pwd_new"].
URL	http://172.16.2.34:8069/web/database/change_password
Method	POST
Attack	
Evidence	<form id="form-duplicate-db" role="form" action="/web/database/duplicate" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 4: "dbname_duplicate" "master_pwd" "new_name"].
URL	http://172.16.2.34:8069/web/database/change_password
Method	POST
Attack	
Evidence	<form id="form_drop_db" role="form" action="/web/database/drop" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following

	HTML form: [Form 5: "dbname_delete" "master_pwd"].
URL	http://172.16.2.34:8069/web/database/change_password
Method	POST
Attack	
Evidence	<form id="form_backup_db" role="form" action="/web/database/backup" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 6: "dbname_backup" "master_pwd"].
URL	http://172.16.2.34:8069/web/database/create
Method	POST
Attack	
Evidence	<form role="form" action="/web/database/create" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "dbname" "load_demo_checkbox" "login" "master_pwd" "password" "phone"].
URL	http://172.16.2.34:8069/web/database/create
Method	POST
Attack	
Evidence	<form id="form_restore_db" role="form" action="/web/database/restore" method="post" enctype="multipart/form-data">
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: "backup_file" "dbname_restore" "master_pwd" "radio_copy_false" "radio_copy_true"].
URL	http://172.16.2.34:8069/web/database/create
Method	POST
Attack	
Evidence	<form id="form_change_pwd" role="form" action="/web/database/change_password" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 3: "master_pwd" "master_pwd_new"].
URL	http://172.16.2.34:8069/web/database/create
Method	POST
Attack	
Evidence	<form id="form-duplicate-db" role="form" action="/web/database/duplicate" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 4: "dbname_duplicate" "master_pwd" "new_name"].
URL	http://172.16.2.34:8069/web/database/create
Method	POST
Attack	
Evidence	<form id="form_drop_db" role="form" action="/web/database/drop" method="post">

Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 5: "dbname_delete" "master_pwd"].
URL	http://172.16.2.34:8069/web/database/create
Method	POST
Attack	
Evidence	<form id="form_backup_db" role="form" action="/web/database/backup" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 6: "dbname_backup" "master_pwd"].
URL	http://172.16.2.34:8069/web/database/drop
Method	POST
Attack	
Evidence	<form role="form" action="/web/database/create" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "dbname" "load_demo_checkbox" "login" "master_pwd" "password" "phone"].
URL	http://172.16.2.34:8069/web/database/drop
Method	POST
Attack	
Evidence	<form id="form_restore_db" role="form" action="/web/database/restore" method="post" enctype="multipart/form-data">
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: "backup_file" "dbname_restore" "master_pwd" "radio_copy_false" "radio_copy_true"].
URL	http://172.16.2.34:8069/web/database/drop
Method	POST
Attack	
Evidence	<form id="form_change_pwd" role="form" action="/web/database/change_password" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 3: "master_pwd" "master_pwd_new"].
URL	http://172.16.2.34:8069/web/database/drop
Method	POST
Attack	
Evidence	<form id="form-duplicate-db" role="form" action="/web/database/duplicate" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 4: "dbname_duplicate" "master_pwd" "new_name"].
URL	http://172.16.2.34:8069/web/database/drop
Method	POST

Attack	
Evidence	<form id="form_drop_db" role="form" action="/web/database/drop" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 5: "dbname_delete" "master_pwd"].
URL	http://172.16.2.34:8069/web/database/drop
Method	POST
Attack	
Evidence	<form id="form_backup_db" role="form" action="/web/database/backup" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 6: "dbname_backup" "master_pwd"].
URL	http://172.16.2.34:8069/web/database/duplicate
Method	POST
Attack	
Evidence	<form role="form" action="/web/database/create" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "dbname" "load_demo_checkbox" "login" "master_pwd" "password" "phone"].
URL	http://172.16.2.34:8069/web/database/duplicate
Method	POST
Attack	
Evidence	<form id="form_restore_db" role="form" action="/web/database/restore" method="post" enctype="multipart/form-data">
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: "backup_file" "dbname_restore" "master_pwd" "radio_copy_false" "radio_copy_true"].
URL	http://172.16.2.34:8069/web/database/duplicate
Method	POST
Attack	
Evidence	<form id="form_change_pwd" role="form" action="/web/database/change_password" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 3: "master_pwd" "master_pwd_new"].
URL	http://172.16.2.34:8069/web/database/duplicate
Method	POST
Attack	
Evidence	<form id="form-duplicate-db" role="form" action="/web/database/duplicate" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 4: "dbname_duplicate" "master_pwd" "new_name"].

URL	http://172.16.2.34:8069/web/database/duplicate
Method	POST
Attack	
Evidence	<form id="form_drop_db" role="form" action="/web/database/drop" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 5: "dbname_delete" "master_pwd"].
URL	http://172.16.2.34:8069/web/database/duplicate
Method	POST
Attack	
Evidence	<form id="form_backup_db" role="form" action="/web/database/backup" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 6: "dbname_backup" "master_pwd"].
URL	http://172.16.2.34:8069/web/database/restore
Method	POST
Attack	
Evidence	<form role="form" action="/web/database/create" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "dbname" "load_demo_checkbox" "login" "master_pwd" "password" "phone"].
URL	http://172.16.2.34:8069/web/database/restore
Method	POST
Attack	
Evidence	<form id="form_restore_db" role="form" action="/web/database/restore" method="post" enctype="multipart/form-data">
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: "backup_file" "dbname_restore" "master_pwd" "radio_copy_false" "radio_copy_true"].
URL	http://172.16.2.34:8069/web/database/restore
Method	POST
Attack	
Evidence	<form id="form_change_pwd" role="form" action="/web/database/change_password" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 3: "master_pwd" "master_pwd_new"].
URL	http://172.16.2.34:8069/web/database/restore
Method	POST
Attack	
Evidence	<form id="form-duplicate-db" role="form" action="/web/database/duplicate" method="post">
	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 4: "dbname_duplicate" "master_pwd" "new_name"].
URL	http://172.16.2.34:8069/web/database/restore
Method	POST
Attack	
Evidence	<form id="form_drop_db" role="form" action="/web/database/drop" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 5: "dbname_delete" "master_pwd"].
URL	http://172.16.2.34:8069/web/database/restore
Method	POST
Attack	
Evidence	<form id="form_backup_db" role="form" action="/web/database/backup" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 6: "dbname_backup" "master_pwd"].
Instances	42
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://172.16.2.34:8069
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/database/manager
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	
Evidence	
Other	

Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/database/backup
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/database/change_password
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/database/create
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/database/drop
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/database/duplicate
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/database/restore
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login

Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	
Evidence	
Other Info	
Instances	15
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	**Cross-Domain Misconfiguration**
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	http://172.16.2.34:8069/web/binary/company_logo
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	1
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14

Plugin Id	10098

Medium	Missing Anti-clickjacking Header
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
URL	http://172.16.2.34:8069/web/database/manager
Method	GET
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/database/backup
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/database/change_password
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/database/create
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/database/drop
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/database/duplicate
Method	POST
Attack	
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/database/restore
Method	POST
Attack	

Evidence	
Other Info	
Instances	7
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	**Vulnerable JS Library**
Description	The identified library jquery, version 3.3.1 is vulnerable.
URL	http://172.16.2.34:8069/web/static/lib/jquery/jquery.js
Method	GET
Attack	
Evidence	* jQuery JavaScript Library v3.3.1
Other Info	CVE-2020-11023 CVE-2020-11022 CVE-2019-11358 CVE-2020-23064
Instances	1
Solution	Please upgrade to the latest version of jquery.
Reference	https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
CWE Id	829
WASC Id	
Plugin Id	10003

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://172.16.2.34:8069
Method	GET
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web
Method	GET
Attack	
Evidence	Set-Cookie: session_id
Other	

Info	
URL	http://172.16.2.34:8069/web/assets/199-59bbeaa/web.assets_common.min.css
Method	GET
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/assets/204-cc89601/web.assets_frontend.min.css
Method	GET
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/assets/205-9760593/web.assets_common_minimal.min.js
Method	GET
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/assets/206-1ab8328/web.assets_frontend_minimal.min.js
Method	GET
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/binary/company_logo
Method	GET
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/database/manager
Method	GET
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/reset_password

Method	GET
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/database/backup
Method	POST
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/database/change_password
Method	POST
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/database/create
Method	POST
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/database/drop
Method	POST
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/database/duplicate
Method	POST

Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/database/restore
Method	POST
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	
Evidence	Set-Cookie: session_id
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	POST
Attack	
Evidence	Set-Cookie: session_id
Other Info	
Instances	21
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	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	http://172.16.2.34:8069
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	

URL	http://172.16.2.34:8069/robots.txt
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/sitemap.xml
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/assets/199-59bbeaa/web.assets_common.min.css
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/assets/204-cc89601/web.assets_frontend.min.css
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/assets/205-9760593/web.assets_common_minimal.min.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/assets/206-1ab8328/web.assets_frontend_minimal.min.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/binary/company_logo
Method	GET

Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/database/manager
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/img/favicon.ico
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/img/logo2.png
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/css/bootstrap.css
Method	GET
Attack	

Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/alert.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/button.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/carousel.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/collapse.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/dropdown.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/index.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/modal.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other	

Info	
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/popover.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/scrollspy.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/tab.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/tooltip.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/util.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/fontawesome/css/font-awesome.css
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/fontawesome/fonts/fontawesome-webfont.woff2?v=4.7.0
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	

URL	http://172.16.2.34:8069/web/static/lib/jquery/jquery.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/lib/popper/popper.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/static/src/public/database_manager.js
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/database/backup
Method	POST
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/database/change_password
Method	POST
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/database/create
Method	POST
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/database/drop
Method	POST

Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/database/duplicate
Method	POST
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/database/restore
Method	POST
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	POST
Attack	
Evidence	Werkzeug/0.16.1 Python/3.8.10
Other Info	
Instances	43
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10036

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://172.16.2.34:8069
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.
URL	http://172.16.2.34:8069/web/binary/company_logo
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.
URL	http://172.16.2.34:8069/web/database/manager
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.
URL	http://172.16.2.34:8069/web/login
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.
URL	http://172.16.2.34:8069/web/reset_password
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.
URL	http://172.16.2.34:8069/web/signup
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.
URL	http://172.16.2.34:8069/web/static/img/favicon.ico
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.
URL	http://172.16.2.34:8069/web/static/img/logo2.png
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.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/css/bootstrap.css
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.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/alert.js
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.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/button.js
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.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/carousel.js
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.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/collapse.js
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.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/dropdown.js
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.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/index.js
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.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/modal.js
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.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/popover.js
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.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/scrollspy.js
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.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/tab.js
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.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/tooltip.js
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.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/util.js
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.
URL	http://172.16.2.34:8069/web/static/lib/fontawesome/css/font-awesome.css
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.
URL	http://172.16.2.34:8069/web/static/lib/fontawesome/fonts/fontawesome-webfont.woff2?v=4.7.0
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.
URL	http://172.16.2.34:8069/web/static/lib/jquery/jquery.js
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.
URL	http://172.16.2.34:8069/web/static/lib/popper/popper.js
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.
URL	http://172.16.2.34:8069/web/static/src/public/database_manager.js
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.
URL	http://172.16.2.34:8069/web/database/backup
Method	POST
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.
URL	http://172.16.2.34:8069/web/database/change_password
Method	POST
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.
URL	http://172.16.2.34:8069/web/database/create
Method	POST
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.
URL	http://172.16.2.34:8069/web/database/drop
Method	POST
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.
URL	http://172.16.2.34:8069/web/database/duplicate
Method	POST
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.
URL	http://172.16.2.34:8069/web/database/restore
Method	POST
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.
URL	http://172.16.2.34:8069/web/login
Method	POST
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.
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
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	34
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://172.16.2.34:8069/web/database/create
Method	POST
Attack	
Evidence	password
Other Info	userParam=login userValue=ZAP passwordParam=password referer=http://172.16.2.34:8069/web/database/manager
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	
Evidence	password
Other Info	userParam=login userValue=ZAP passwordParam=password referer=http://172.16.2.34:8069/web/login csrfToken=csrf_token
Instances	2
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	**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://172.16.2.34:8069
Method	GET
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "<script id="web.layout.odooscript" type="text/javascript"> var odoo = { csrf_token: '', see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/assets/205-9760593/web.assets_common_minimal.min.js
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: "missing=odoo.__DEBUG__.getMissingJobs();failed=odoo.__DEBUG__.getFailedJobs();var unloaded=Object.keys(debugJobs).map(function(k", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/assets/205-9760593/web.assets_common_minimal.min.js
Method	GET
Attack	
Evidence	from
Other	The following pattern was used: \bFROM\b and was detected 3 times, the first in the element starting with: "var odoo=window.odoo;var debug=odoo.debug;var

Info	didLogInfoResolve;var didLogInfoPromise=new Promise(function(resolve){didLogInfoRe", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "<script id="web.layout.odooscript" type="text/javascript"> var odoo = { csrf_token: ", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "<script id="web.layout.odooscript" type="text/javascript"> var odoo = { csrf_token: ", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "<script id="web.layout.odooscript" type="text/javascript"> var odoo = { csrf_token: ", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/carousel.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 2 times, the first in the element starting with: " from: fromIndex,", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/carousel.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: " // would stop cycling until user tapped out of it;", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/modal.js
Method	GET
Attack	
Evidence	todo
Other Info	The following pattern was used: \bTODO\b and was detected in the element starting with: " // todo (fat): these should probably be refactored out of modal.js", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/scrollspy.js
Method	GET
Attack	

Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected in the element starting with: " // TODO (fat): remove sketch reliance on jQuery position/offset", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/bootstrap/js/util.js
Method	GET
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected in the element starting with: " // TODO: Remove in v5", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/jquery/jquery.js
Method	GET
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 7 times, the first in the element starting with: " // We allow this because of a bug in IE8/9 that throws an error", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/jquery/jquery.js
Method	GET
Attack	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected 7 times, the first in the element starting with: " // See https://bugs.jquery.com/ticket/13378", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/jquery/jquery.js
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 48 times, the first in the element starting with: " // Return just the one element from the set", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/jquery/jquery.js
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 8 times, the first in the element starting with: " // IE8 throws error here and will not see later tests", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/jquery/jquery.js
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 2 times, the first in the element starting with: " // want to query the value if it is a CSS custom property", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/jquery/jquery.js

Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 18 times, the first in the element starting with: " select,", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/jquery/jquery.js
Method	GET
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 4 times, the first in the element starting with: " // TODO: identify versions", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/jquery/jquery.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 9 times, the first in the element starting with: " // Can be adjusted by the user", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/jquery/jquery.js
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected 2 times, the first in the element starting with: " username: null,", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.34:8069/web/static/lib/jquery/jquery.js
Method	GET
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 9 times, the first in the element starting with: " // For CommonJS and CommonJS-like environments where a proper `window`", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/popper/popper.js
Method	GET
Attack	
Evidence	FROM
Other Info	The following pattern was used: \bFROM\b and was detected 15 times, the first in the element starting with: " * LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,", see evidence field for the suspicious comment /snippet.
URL	http://172.16.2.34:8069/web/static/lib/popper/popper.js
Method	GET
Attack	
Evidence	query
Other	The following pattern was used: \bQUERY\b and was detected in the element starting with:

Info	" // if the arrowElement isn't a query selector we must check that the", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/popper/popper.js
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in the element starting with: " // remove the popper if user explicity asked for the deletion on destroy", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/lib/popper/popper.js
Method	GET
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 4 times, the first in the element starting with: " // In cases where the parent is fixed, we must ignore negative scroll in offset calc", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/static/src/public/database_manager.js
Method	GET
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected 3 times, the first in the element starting with: " // db modal", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "<script id="web.layout.odooscript" type="text/javascript"> var odoo = { csrf_token: ", see evidence field for the suspicious comment/snippet.
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "<script id="web.layout.odooscript" type="text/javascript"> var odoo = { csrf_token: ", see evidence field for the suspicious comment/snippet.
Instances	28
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	**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://172.16.2.34:8069
Method	GET
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069
Method	GET
Attack	
Evidence	9168a5787c7665615bb8ca7d6acafcae3275f473
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web
Method	GET
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/assets/199-59bbeaa/web.assets_common.min.css
Method	GET
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/assets/204-cc89601/web.assets_frontend.min.css
Method	GET
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/assets/205-9760593/web.assets_common_minimal.min.js
Method	GET
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/assets/206-1ab8328/web.assets_frontend_minimal.min.js
Method	GET
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id

URL	http://172.16.2.34:8069/web/binary/company_logo
Method	GET
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/database/manager
Method	GET
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/database/backup
Method	POST
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/database/change_password
Method	POST

Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/database/create
Method	POST
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/database/drop
Method	POST
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/database/duplicate
Method	POST
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/database/restore
Method	POST
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/signup
Method	POST
Attack	

Evidence	d621361f1eb6100358782197c45fef46669aaf1f
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
URL	http://172.16.2.34:8069/web/database/drop
Method	POST
Attack	
Evidence	5f7ba2c1cf98897a2dcfbf8cd67f8bb8e530126e
Other Info	cookie:session_id
Instances	24
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 Agent Fuzzer**
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	http://172.16.2.34:8069
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://172.16.2.34:8069
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069

Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://172.16.2.34:8069
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://172.16.2.34:8069
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://172.16.2.34:8069
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://172.16.2.34:8069
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://172.16.2.34:8069

Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://172.16.2.34:8069
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web
Method	GET

Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET

Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)

Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4

Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	

Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	

Other Info	
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other	

Info	
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web?db=odoo
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	

URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	

URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/login
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password

Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	

URL	http://172.16.2.34:8069/web/reset_password
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup

Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://172.16.2.34:8069/web/signup
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	108
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

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://172.16.2.34:8069/web/database/backup
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://172.16.2.34:8069/web /database/backup appears to include user input in: a(n) [option] tag [value] attribute The user input found was: backup_format=dump The user-controlled value was: dump
URL	http://172.16.2.34:8069/web/database/create
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://172.16.2.34:8069/web /database/create appears to include user input in: a(n) [option] tag [value] attribute The user input found was: country_code=af The user-controlled value was: af
URL	http://172.16.2.34:8069/web/database/create
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://172.16.2.34:8069/web /database/create appears to include user input in: a(n) [option] tag [value] attribute The user input found was: lang=en The user-controlled value was: en_au
URL	http://172.16.2.34:8069/web/database/create
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://172.16.2.34:8069/web /database/create appears to include user input in: a(n) [option] tag [value] attribute The user input found was: lang=en The user-controlled value was: en_ca
URL	http://172.16.2.34:8069/web/database/create
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://172.16.2.34:8069/web /database/create appears to include user input in: a(n) [option] tag [value] attribute The user input found was: lang=en The user-controlled value was: en_gb
URL	http://172.16.2.34:8069/web/database/create
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://172.16.2.34:8069/web/database/create appears to include user input in: a(n) [option] tag [value] attribute The user input found was: lang=en The user-controlled value was: en_in
URL	http://172.16.2.34:8069/web/database/create
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://172.16.2.34:8069/web/database/create appears to include user input in: a(n) [option] tag [value] attribute The user input found was: lang=en The user-controlled value was: en_us
URL	http://172.16.2.34:8069/web/database/restore
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://172.16.2.34:8069/web/database/restore appears to include user input in: a(n) [input] tag [value] attribute The user input found was: copy=true The user-controlled value was: true
URL	http://172.16.2.34:8069/web/database/restore
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://172.16.2.34:8069/web/database/restore appears to include user input in: a(n) [span] tag [aria-hidden] attribute The user input found was: copy=true The user-controlled value was: true
URL	http://172.16.2.34:8069/web/login
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://172.16.2.34:8069/web/login appears to include user input in: a(n) [input] tag [value] attribute The user input found was: csrf_token=1c0aa63afdf0e99154c14de9797fb741147df604o1733339153 The user-controlled value was: 1c0aa63afdf0e99154c14de9797fb741147df604o1733339153
URL	http://172.16.2.34:8069/web/login
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://172.16.2.34:8069/web/login appears to include user input in: a(n) [input] tag [value] attribute The user input found was: login=ZAP The user-controlled value was: zap
URL	http://172.16.2.34:8069/web/login
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://172.16.2.34:8069/web/login appears to include user input in: a(n) [input] tag [value] attribute The user input found was: password=ZAP The user-controlled value was: zap
URL	http://172.16.2.34:8069/web/reset_password
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://172.16.2.34:8069/web /reset_password appears to include user input in: a(n) [input] tag [value] attribute The user input found was: csrf_token=1c0aa63afdf0e99154c14de9797fb741147df604o1733339153 The user-controlled value was: 1c0aa63afdf0e99154c14de9797fb741147df604o1733339153
URL	http://172.16.2.34:8069/web/reset_password
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://172.16.2.34:8069/web /reset_password appears to include user input in: a(n) [input] tag [value] attribute The user input found was: login=ZAP The user-controlled value was: zap
Instances	14
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