



# OWASP ZAP Scan Report

Target: http://testphp.vulnweb.com

All scanned sites: http://testphp.vulnweb.com

Javascript included from: http://testphp.vulnweb.com

Generated on Tue, 23 Sept 2025 22:46:56

ZAP Version: 2.16.1

## Summary of Alerts

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

## Alerts

Name	Risk Level	Number of Instances
<a href="#">Absence of Anti-CSRF Tokens</a>	Medium	40
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	48
<a href="#">Missing Anti-clickjacking Header</a>	Medium	44
<a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s).</a>	Low	62
<a href="#">Server Leaks Version Information via "Server" HTTP Response Header Field</a>	Low	75
<a href="#">X-Content-Type-Options Header Missing</a>	Low	69
<a href="#">Authentication Request Identified</a>	Informational	1
<a href="#">Charset Mismatch (Header Versus Meta Content-Type Charset).</a>	Informational	31
<a href="#">User Controllable HTML Element Attribute (Potential XSS).</a>	Informational	3

## Passing Rules

Name	Rule Type	Threshold	Strength
<a href="#">Session Management Response Identified</a>	Passive	MEDIUM	-
<a href="#">Verification Request Identified</a>	Passive	MEDIUM	-
<a href="#">Private IP Disclosure</a>	Passive	MEDIUM	-
<a href="#">Session ID in URL Rewrite</a>	Passive	MEDIUM	-
<a href="#">Script Served From Malicious Domain (polyfill).</a>	Passive	MEDIUM	-
<a href="#">ZAP is Out of Date</a>	Passive	MEDIUM	-

<a href="#">Insecure JSF ViewState</a>	Passive	MEDIUM	-
<a href="#">Vulnerable JS Library (Powered by Retire.js)</a>	Passive	MEDIUM	-
<a href="#">Cookie No HttpOnly Flag</a>	Passive	MEDIUM	-
<a href="#">Cookie Without Secure Flag</a>	Passive	MEDIUM	-
<a href="#">Re-examine Cache-control Directives</a>	Passive	MEDIUM	-
<a href="#">Cross-Domain JavaScript Source File Inclusion</a>	Passive	MEDIUM	-
<a href="#">Content-Type Header Missing</a>	Passive	MEDIUM	-
<a href="#">Application Error Disclosure</a>	Passive	MEDIUM	-
<a href="#">Information Disclosure - Debug Error Messages</a>	Passive	MEDIUM	-
<a href="#">Information Disclosure - Sensitive Information in URL</a>	Passive	MEDIUM	-
<a href="#">Information Disclosure - Sensitive Information in HTTP Referrer Header</a>	Passive	MEDIUM	-
<a href="#">Information Disclosure - Suspicious Comments</a>	Passive	MEDIUM	-
<a href="#">Off-site Redirect</a>	Passive	MEDIUM	-
<a href="#">Cookie Poisoning</a>	Passive	MEDIUM	-
<a href="#">User Controllable Charset</a>	Passive	MEDIUM	-
<a href="#">WSDL File Detection</a>	Passive	MEDIUM	-
<a href="#">Loosely Scoped Cookie</a>	Passive	MEDIUM	-
<a href="#">Viewstate</a>	Passive	MEDIUM	-
<a href="#">Directory Browsing</a>	Passive	MEDIUM	-
<a href="#">Heartbleed OpenSSL Vulnerability (Indicative)</a>	Passive	MEDIUM	-
<a href="#">Strict-Transport-Security Header</a>	Passive	MEDIUM	-
<a href="#">X-Backend-Server Header Information Leak</a>	Passive	MEDIUM	-
<a href="#">Secure Pages Include Mixed Content</a>	Passive	MEDIUM	-
<a href="#">HTTP to HTTPS Insecure Transition in Form Post</a>	Passive	MEDIUM	-
<a href="#">HTTPS to HTTP Insecure Transition in Form Post</a>	Passive	MEDIUM	-
<a href="#">User Controllable JavaScript Event (XSS)</a>	Passive	MEDIUM	-
<a href="#">Big Redirect Detected (Potential Sensitive Information Leak)</a>	Passive	MEDIUM	-
<a href="#">Retrieved from Cache</a>	Passive	MEDIUM	-
<a href="#">X-ChromeLogger-Data (XCOLD) Header Information Leak</a>	Passive	MEDIUM	-
<a href="#">Cookie without SameSite Attribute</a>	Passive	MEDIUM	-
<a href="#">CSP</a>	Passive	MEDIUM	-
<a href="#">X-Debug-Token Information Leak</a>	Passive	MEDIUM	-
<a href="#">Username Hash Found</a>	Passive	MEDIUM	-
<a href="#">X-AspNet-Version Response Header</a>	Passive	MEDIUM	-
<a href="#">PII Disclosure</a>	Passive	MEDIUM	-
<a href="#">Script Passive Scan Rules</a>	Passive	MEDIUM	-
<a href="#">Stats Passive Scan Rule</a>	Passive	MEDIUM	-
<a href="#">Timestamp Disclosure</a>	Passive	MEDIUM	-
<a href="#">Hash Disclosure</a>	Passive	MEDIUM	-
<a href="#">Cross-Domain Misconfiguration</a>	Passive	MEDIUM	-
<a href="#">Weak Authentication Method</a>	Passive	MEDIUM	-
<a href="#">Reverse Tabnabbing</a>	Passive	MEDIUM	-
<a href="#">Modern Web Application</a>	Passive	MEDIUM	-

Alert Detail

Medium	Absence of Anti-CSRF Tokens
Description	<p>No Anti-CSRF tokens were found in a HTML submission form.</p> <p>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.</p> <p>CSRF attacks are effective in a number of situations, including:</p> <ul style="list-style-type: none"><li>* The victim has an active session on the target site.</li><li>* The victim is authenticated via HTTP auth on the target site.</li><li>* The victim is on the same local network as the target site.</li></ul> <p>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.</p>
URL	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wponce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
Request Header	GET http://testphp.vulnweb.com/ HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:12 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 4958
Response Body (excerpt)	tent_rgn" --> <div id="content"> <h2 id="pageName">welcome to our page</h2> <div class="story"> <h3>Test site for Acunetix WVS.</h3> </div> </div> <!-- InstanceEndEditable --> <!--end content -->

	<pre>&lt;div id="navBar"&gt;   &lt;div id="search"&gt;     &lt;form action="search.php?test=query" method="post"&gt;       &lt;label&gt;search art&lt;/label&gt;       &lt;input name="searchFor" type="text" size="10"&gt;       &lt;input name="goButton" type="submit" value="go"&gt;     &lt;/form&gt;   &lt;/div&gt;   &lt;div id="sectionLinks"&gt;     &lt;ul&gt;       &lt;li&gt;&lt;a href="categories.php"&gt;Browse cat</pre>
URL	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=1">http://testphp.vulnweb.com/artists.php?artist=1</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=2">http://testphp.vulnweb.com/artists.php?artist=2</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=3">http://testphp.vulnweb.com/artists.php?artist=3</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wponce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/categories.php">http://testphp.vulnweb.com/categories.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wponce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/disclaimer.php">http://testphp.vulnweb.com/disclaimer.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wponce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="" method="post" name="faddentry">
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, data[_Token][key], _wponce] was found in the following HTML form: [Form 1: "name" "submit" ].
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wponce] was found in the following HTML form: [Form 2: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/index.php">http://testphp.vulnweb.com/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wponce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=1">http://testphp.vulnweb.com/listproducts.php?artist=1</a>
Method	GET

Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=2">http://testphp.vulnweb.com/listproducts.php?artist=2</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=3">http://testphp.vulnweb.com/listproducts.php?artist=3</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=1">http://testphp.vulnweb.com/listproducts.php?cat=1</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=2">http://testphp.vulnweb.com/listproducts.php?cat=2</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=3">http://testphp.vulnweb.com/listproducts.php?cat=3</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form

	1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=4">http://testphp.vulnweb.com/listproducts.php?cat=4</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/login.php">http://testphp.vulnweb.com/login.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form name="loginform" method="post" action="userinfo.php">
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "pass" "uname" ].
URL	<a href="http://testphp.vulnweb.com/login.php">http://testphp.vulnweb.com/login.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 2: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/product.php?pic=1">http://testphp.vulnweb.com/product.php?pic=1</a>
Method	GET
Parameter	
Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "addcart" "price" ].
URL	<a href="http://testphp.vulnweb.com/product.php?pic=1">http://testphp.vulnweb.com/product.php?pic=1</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 2: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/product.php?pic=2">http://testphp.vulnweb.com/product.php?pic=2</a>
Method	GET
Parameter	

Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 1: "addcart" "price" ].
URL	<a href="http://testphp.vulnweb.com/product.php?pic=2">http://testphp.vulnweb.com/product.php?pic=2</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 2: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/product.php?pic=3">http://testphp.vulnweb.com/product.php?pic=3</a>
Method	GET
Parameter	
Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 1: "addcart" "price" ].
URL	<a href="http://testphp.vulnweb.com/product.php?pic=3">http://testphp.vulnweb.com/product.php?pic=3</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 2: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/product.php?pic=4">http://testphp.vulnweb.com/product.php?pic=4</a>
Method	GET
Parameter	
Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 1: "addcart" "price" ].
URL	<a href="http://testphp.vulnweb.com/product.php?pic=4">http://testphp.vulnweb.com/product.php?pic=4</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 2: "goButton" "searchFor" ].



URL	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Method	GET
Parameter	
Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 1: "addcart" "price" ].
URL	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 2: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>
Method	GET
Parameter	
Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 1: "addcart" "price" ].
URL	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 2: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	
Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 1: "addcart" "price" ].
URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	
Attack	

Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wptime] was found in the following HTML form: [Form 2: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form name="form1" method="post" action="/secured/newuser.php">
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, data[_Token][key], _wptime] was found in the following HTML form: [Form 1: "signup" "ucc" "uemail" "upass" "upass2" "uphone" "urname" "uuname" ].
URL	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wptime] was found in the following HTML form: [Form 2: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	POST
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wptime] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	
Attack	
Evidence	<form action="" method="post" name="faddentry">
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, data[_Token][key], _wptime] was found in the following HTML form: [Form 1: "name" "submit" ].
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token][key], _wptime] was found in the following HTML form: [Form 2: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>

Method	POST
Parameter	
Attack	
Evidence	<form action="search.php?test=query" 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, data[_Token]][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
Instances	40
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	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html</a> <a href="https://cwe.mitre.org/data/definitions/352.html">https://cwe.mitre.org/data/definitions/352.html</a>
CWE Id	<a href="#">352</a>
WASC Id	9
Plugin Id	<a href="#">10202</a>

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	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
Request Header	GET http://testphp.vulnweb.com/ HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:12 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 4958
Response Body (truncated)	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLOutsideIsLocked="false" --> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">  <!-- InstanceBeginEditable name="document_title_rgn" --> <title>Home of Acunetix Art</title> <!-- InstanceEndEditable --> <link rel="stylesheet" href="style.css" type="text/css"> <!-- InstanceBeginEditab...(truncated)
URL	<a href="http://testphp.vulnweb.com/AJAX/index.php">http://testphp.vulnweb.com/AJAX/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=1">http://testphp.vulnweb.com/artists.php?artist=1</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	<a href="http://testphp.vulnweb.com/artists.php?artist=2">http://testphp.vulnweb.com/artists.php?artist=2</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=3">http://testphp.vulnweb.com/artists.php?artist=3</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/categories.php">http://testphp.vulnweb.com/categories.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/disclaimer.php">http://testphp.vulnweb.com/disclaimer.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/high">http://testphp.vulnweb.com/high</a>
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/hpp/">http://testphp.vulnweb.com/hpp/</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/hpp/?pp=12">http://testphp.vulnweb.com/hpp/?pp=12</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/hpp/params.php?p=valid&amp;pp=12">http://testphp.vulnweb.com/hpp/params.php?p=valid&amp;pp=12</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/index.php">http://testphp.vulnweb.com/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=1">http://testphp.vulnweb.com/listproducts.php?artist=1</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=2">http://testphp.vulnweb.com/listproducts.php?artist=2</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=3">http://testphp.vulnweb.com/listproducts.php?artist=3</a>
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=1">http://testphp.vulnweb.com/listproducts.php?cat=1</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=2">http://testphp.vulnweb.com/listproducts.php?cat=2</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=3">http://testphp.vulnweb.com/listproducts.php?cat=3</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=4">http://testphp.vulnweb.com/listproducts.php?cat=4</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/login.php">http://testphp.vulnweb.com/login.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html</a>
Method	GET
Parameter	
Attack	



Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/privacy.php">http://testphp.vulnweb.com/privacy.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=1">http://testphp.vulnweb.com/product.php?pic=1</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=2">http://testphp.vulnweb.com/product.php?pic=2</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=3">http://testphp.vulnweb.com/product.php?pic=3</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=4">http://testphp.vulnweb.com/product.php?pic=4</a>
Method	GET

Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/robots.txt">http://testphp.vulnweb.com/robots.txt</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/sitemap.xml">http://testphp.vulnweb.com/sitemap.xml</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	

URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/secured/newuser.php">http://testphp.vulnweb.com/secured/newuser.php</a>
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
Instances	48
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	<a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP">https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP</a> <a href="https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html</a> <a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://w3c.github.io/webappsec-csp/">https://w3c.github.io/webappsec-csp/</a> <a href="https://web.dev/articles/csp">https://web.dev/articles/csp</a> <a href="https://caniuse.com/#feat=contentsecuritypolicy">https://caniuse.com/#feat=contentsecuritypolicy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10038</a>

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	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Method	GET
Parameter	x-frame-options

Attack	
Evidence	
Other Info	
Request Header	GET http://testphp.vulnweb.com/ HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:12 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 4958
Response Body (truncated)	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" --> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">  <!-- InstanceBeginEditable name="document_title_rgn" --> <title>Home of Acunetix Art</title> <!-- InstanceEndEditable --> <link rel="stylesheet" href="style.css" type="text/css"> <!-- InstanceBeginEditab...(truncated)
URL	<a href="http://testphp.vulnweb.com/AJAX/index.php">http://testphp.vulnweb.com/AJAX/index.php</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=1">http://testphp.vulnweb.com/artists.php?artist=1</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	

Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=2">http://testphp.vulnweb.com/artists.php?artist=2</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=3">http://testphp.vulnweb.com/artists.php?artist=3</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/categories.php">http://testphp.vulnweb.com/categories.php</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/disclaimer.php">http://testphp.vulnweb.com/disclaimer.php</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/hpp/">http://testphp.vulnweb.com/hpp/</a>
Method	GET
Parameter	x-frame-options

Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/hpp/?pp=12">http://testphp.vulnweb.com/hpp/?pp=12</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/hpp/params.php?p=valid&amp;pp=12">http://testphp.vulnweb.com/hpp/params.php?p=valid&amp;pp=12</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/index.php">http://testphp.vulnweb.com/index.php</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=1">http://testphp.vulnweb.com/listproducts.php?artist=1</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=2">http://testphp.vulnweb.com/listproducts.php?artist=2</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=3">http://testphp.vulnweb.com/listproducts.php?artist=3</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=1">http://testphp.vulnweb.com/listproducts.php?cat=1</a>

Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=2">http://testphp.vulnweb.com/listproducts.php?cat=2</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=3">http://testphp.vulnweb.com/listproducts.php?cat=3</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=4">http://testphp.vulnweb.com/listproducts.php?cat=4</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/login.php">http://testphp.vulnweb.com/login.php</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	

Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html</a>
Method	GET
Parameter	x-frame-options



Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=1">http://testphp.vulnweb.com/product.php?pic=1</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=2">http://testphp.vulnweb.com/product.php?pic=2</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=3">http://testphp.vulnweb.com/product.php?pic=3</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=4">http://testphp.vulnweb.com/product.php?pic=4</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>

Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/secured/newuser.php">http://testphp.vulnweb.com/secured/newuser.php</a>
Method	POST
Parameter	x-frame-options
Attack	
Evidence	

Other Info	
Instances	44
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	<a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options</a>
CWE Id	<a href="#">1021</a>
WASC Id	15
Plugin Id	<a href="#">10020</a>

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	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
Request Header	GET http://testphp.vulnweb.com/ HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:12 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive <b>X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1</b> content-length: 4958
Response Body (truncated)	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLOutsideIsLocked="false" --> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">  <!-- InstanceBeginEditable name="document_title_rgn" --> <title>Home of Acunetix Art</title> <!-- InstanceEndEditable --> <link rel="stylesheet" href="style.css" type="text/css"> <!-- InstanceBeginEditab...(truncated)
URL	<a href="http://testphp.vulnweb.com/AJAX/index.php">http://testphp.vulnweb.com/AJAX/index.php</a>
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=1">http://testphp.vulnweb.com/artists.php?artist=1</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=2">http://testphp.vulnweb.com/artists.php?artist=2</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=3">http://testphp.vulnweb.com/artists.php?artist=3</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/categories.php">http://testphp.vulnweb.com/categories.php</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	

URL	<a href="http://testphp.vulnweb.com/disclaimer.php">http://testphp.vulnweb.com/disclaimer.php</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/hpp/">http://testphp.vulnweb.com/hpp/</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/hpp/?pp=12">http://testphp.vulnweb.com/hpp/?pp=12</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/hpp/params.php?p=valid&amp;pp=12">http://testphp.vulnweb.com/hpp/params.php?p=valid&amp;pp=12</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/index.php">http://testphp.vulnweb.com/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=1">http://testphp.vulnweb.com/listproducts.php?artist=1</a>
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=2">http://testphp.vulnweb.com/listproducts.php?artist=2</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=3">http://testphp.vulnweb.com/listproducts.php?artist=3</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=1">http://testphp.vulnweb.com/listproducts.php?cat=1</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=2">http://testphp.vulnweb.com/listproducts.php?cat=2</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=3">http://testphp.vulnweb.com/listproducts.php?cat=3</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=4">http://testphp.vulnweb.com/listproducts.php?cat=4</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/login.php">http://testphp.vulnweb.com/login.php</a>
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	

URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/privacy.php">http://testphp.vulnweb.com/privacy.php</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=1">http://testphp.vulnweb.com/product.php?pic=1</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=2">http://testphp.vulnweb.com/product.php?pic=2</a>
Method	GET
Parameter	
Attack	



Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=3">http://testphp.vulnweb.com/product.php?pic=3</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=4">http://testphp.vulnweb.com/product.php?pic=4</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'">http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg</a>
Method	GET

Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	

URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	

Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/userinfo.php">http://testphp.vulnweb.com/userinfo.php</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/secured/newuser.php">http://testphp.vulnweb.com/secured/newuser.php</a>
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/userinfo.php">http://testphp.vulnweb.com/userinfo.php</a>
Method	POST

Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
Instances	62
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	<a href="https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework">https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework</a> <a href="https://www.troyhunt.com/shhh-dont-let-your-response-headers/">https://www.troyhunt.com/shhh-dont-let-your-response-headers/</a>
CWE Id	<a href="#">497</a>
WASC Id	13
Plugin Id	<a href="#">10037</a>

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	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
Request Header	GET http://testphp.vulnweb.com/ HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Server: <b>nginx/1.19.0</b> Date: Tue, 23 Sep 2025 22:46:12 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 4958
Response Body (truncated)	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLOutsideIsLocked="false" --> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">  <!-- InstanceBeginEditable name="document_title_rgn" --> <title>Home of Acunetix Art</title> <!-- InstanceEndEditable --> <link rel="stylesheet" href="style.css" type="text/css"> <!-- InstanceBeginEditab...(truncated)

URL	<a href="http://testphp.vulnweb.com/AJAX/index.php">http://testphp.vulnweb.com/AJAX/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/AJAX/styles.css">http://testphp.vulnweb.com/AJAX/styles.css</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=1">http://testphp.vulnweb.com/artists.php?artist=1</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=2">http://testphp.vulnweb.com/artists.php?artist=2</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=3">http://testphp.vulnweb.com/artists.php?artist=3</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	GET
Parameter	
Attack	

Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/categories.php">http://testphp.vulnweb.com/categories.php</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/disclaimer.php">http://testphp.vulnweb.com/disclaimer.php</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/favicon.ico">http://testphp.vulnweb.com/favicon.ico</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/Flash/add.swf">http://testphp.vulnweb.com/Flash/add.swf</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/high">http://testphp.vulnweb.com/high</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/hpp/">http://testphp.vulnweb.com/hpp/</a>
Method	GET

Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/hpp/?pp=12">http://testphp.vulnweb.com/hpp/?pp=12</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/hpp/params.php?p=valid&amp;pp=12">http://testphp.vulnweb.com/hpp/params.php?p=valid&amp;pp=12</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/images/logo.gif">http://testphp.vulnweb.com/images/logo.gif</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/images/remark.gif">http://testphp.vulnweb.com/images/remark.gif</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/index.php">http://testphp.vulnweb.com/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=1">http://testphp.vulnweb.com/listproducts.php?artist=1</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	



URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=2">http://testphp.vulnweb.com/listproducts.php?artist=2</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=3">http://testphp.vulnweb.com/listproducts.php?artist=3</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=1">http://testphp.vulnweb.com/listproducts.php?cat=1</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=2">http://testphp.vulnweb.com/listproducts.php?cat=2</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=3">http://testphp.vulnweb.com/listproducts.php?cat=3</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=4">http://testphp.vulnweb.com/listproducts.php?cat=4</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/login.php">http://testphp.vulnweb.com/login.php</a>
Method	GET
Parameter	
Attack	

Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/</a>
Method	GET

Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg">http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg">http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg">http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	

URL	<a href="http://testphp.vulnweb.com/privacy.php">http://testphp.vulnweb.com/privacy.php</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=1">http://testphp.vulnweb.com/product.php?pic=1</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=2">http://testphp.vulnweb.com/product.php?pic=2</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=3">http://testphp.vulnweb.com/product.php?pic=3</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=4">http://testphp.vulnweb.com/product.php?pic=4</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>
Method	GET
Parameter	
Attack	

Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/robots.txt">http://testphp.vulnweb.com/robots.txt</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/secured/style.css">http://testphp.vulnweb.com/secured/style.css</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'">http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg</a>
Method	GET

Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	

URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/sitemap.xml">http://testphp.vulnweb.com/sitemap.xml</a>
Method	GET
Parameter	
Attack	

Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/style.css">http://testphp.vulnweb.com/style.css</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/userinfo.php">http://testphp.vulnweb.com/userinfo.php</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	POST
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Method	POST
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/secured/newuser.php">http://testphp.vulnweb.com/secured/newuser.php</a>
Method	POST
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/userinfo.php">http://testphp.vulnweb.com/userinfo.php</a>
Method	POST



Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
Instances	75
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	<a href="https://httpd.apache.org/docs/current/mod/core.html#servertokens">https://httpd.apache.org/docs/current/mod/core.html#servertokens</a> <a href="https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)">https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)</a> <a href="https://www.troyhunt.com/shhh-dont-let-your-response-headers/">https://www.troyhunt.com/shhh-dont-let-your-response-headers/</a>
CWE Id	<a href="#">497</a>
WASC Id	13
Plugin Id	<a href="#">10036</a>

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	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Method	GET
Parameter	x-content-type-options
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.
Request Header	GET http://testphp.vulnweb.com/ HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:12 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 4958

Response Body (truncated)	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLOutsideIsLocked="false" --> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">  <!-- InstanceBeginEditable name="document_title_rgn" --> <title>Home of Acunetix Art</title> <!-- InstanceEndEditable --> <link rel="stylesheet" href="style.css" type="text/css"> <!-- InstanceBeginEditab...(truncated)
URL	<a href="http://testphp.vulnweb.com/AJAX/index.php">http://testphp.vulnweb.com/AJAX/index.php</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/AJAX/styles.css">http://testphp.vulnweb.com/AJAX/styles.css</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/artists.php?artist=1">http://testphp.vulnweb.com/artists.php?artist=1</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/artists.php?artist=2">http://testphp.vulnweb.com/artists.php?artist=2</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/artists.php?artist=3">http://testphp.vulnweb.com/artists.php?artist=3</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/categories.php">http://testphp.vulnweb.com/categories.php</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/disclaimer.php">http://testphp.vulnweb.com/disclaimer.php</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/favicon.ico">http://testphp.vulnweb.com/favicon.ico</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/Flash/add.swf">http://testphp.vulnweb.com/Flash/add.swf</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/hpp/">http://testphp.vulnweb.com/hpp/</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/hpp/?pp=12">http://testphp.vulnweb.com/hpp/?pp=12</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/hpp/params.php?p=valid&amp;pp=12">http://testphp.vulnweb.com/hpp/params.php?p=valid&amp;pp=12</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/images/logo.gif">http://testphp.vulnweb.com/images/logo.gif</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/images/remark.gif">http://testphp.vulnweb.com/images/remark.gif</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/index.php">http://testphp.vulnweb.com/index.php</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/listproducts.php?artist=1">http://testphp.vulnweb.com/listproducts.php?artist=1</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/listproducts.php?artist=2">http://testphp.vulnweb.com/listproducts.php?artist=2</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/listproducts.php?artist=3">http://testphp.vulnweb.com/listproducts.php?artist=3</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/listproducts.php?cat=1">http://testphp.vulnweb.com/listproducts.php?cat=1</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/listproducts.php?cat=2">http://testphp.vulnweb.com/listproducts.php?cat=2</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/listproducts.php?cat=3">http://testphp.vulnweb.com/listproducts.php?cat=3</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/listproducts.php?cat=4">http://testphp.vulnweb.com/listproducts.php?cat=4</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/login.php">http://testphp.vulnweb.com/login.php</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/">http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg">http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg">http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg">http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html">http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/product.php?pic=1">http://testphp.vulnweb.com/product.php?pic=1</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/product.php?pic=2">http://testphp.vulnweb.com/product.php?pic=2</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/product.php?pic=3">http://testphp.vulnweb.com/product.php?pic=3</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/product.php?pic=4">http://testphp.vulnweb.com/product.php?pic=4</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/secured/style.css">http://testphp.vulnweb.com/secured/style.css</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'">http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&amp;size=160</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&amp;size=160</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&amp;size=160</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&amp;size=160</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&amp;size=160</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&amp;size=160</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&amp;size=160</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/style.css">http://testphp.vulnweb.com/style.css</a>
Method	GET
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	POST
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Method	POST
Parameter	x-content-type-options
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	<a href="http://testphp.vulnweb.com/secured/newuser.php">http://testphp.vulnweb.com/secured/newuser.php</a>
Method	POST
Parameter	x-content-type-options
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	69
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	<a href="https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)">https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)</a> <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10021</a>

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	<a href="http://testphp.vulnweb.com/secured/newuser.php">http://testphp.vulnweb.com/secured/newuser.php</a>
Method	POST
Parameter	uemail
Attack	
Evidence	upass
Other Info	userParam=uemail userValue=ZAP passwordParam=upass referer=http://testphp.vulnweb.com/signup.php

Request Header	POST http://testphp.vulnweb.com/secured/newuser.php HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache content-type: application/x-www-form-urlencoded referer: http://testphp.vulnweb.com/signup.php content-length: 96
Request Body	uuname=ZAP&upass=ZAP&upass2=ZAP&urname=ZAP&ucc=ZAP&uemail=ZAP&uphone=ZAP&uaddress=&signup=signup
Response Header	HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:13 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 733
Response Body (truncated)	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <html> <head> <title>add new user</title> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"> <link href="style.css" rel="stylesheet" type="text/css"> </head> <body> <div id="masthead"> <h1 id="siteName">ACUNETIX ART</h1> </div> <div id="content"> <p>You have been introduced to our database with the above informations:</p><ul><li>Username: ZAP</li><li>Pass w...(truncated)
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	<a href="https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/">https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10111</a>
Informational	Charset Mismatch (Header Versus Meta Content-Type Charset)
Description	<p>This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set.</p> <p>An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.</p>
URL	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Method	GET
Parameter	
Attack	
Evidence	

Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
Request Header	GET http://testphp.vulnweb.com/ HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:12 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 4958
Response Body (truncated)	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLOIsLocked="false" --> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">  <!-- InstanceBeginEditable name="document_title_rgn" --> <title>Home of Acunetix Art</title> <!-- InstanceEndEditable --> <link rel="stylesheet" href="style.css" type="text/css"> <!-- InstanceBeginEditab...(truncated)
URL	<a href="http://testphp.vulnweb.com/AJAX/index.php">http://testphp.vulnweb.com/AJAX/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-1] do not match.
URL	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=1">http://testphp.vulnweb.com/artists.php?artist=1</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=2">http://testphp.vulnweb.com/artists.php?artist=2</a>

Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=3">http://testphp.vulnweb.com/artists.php?artist=3</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/categories.php">http://testphp.vulnweb.com/categories.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/disclaimer.php">http://testphp.vulnweb.com/disclaimer.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/index.php">http://testphp.vulnweb.com/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	



Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=1">http://testphp.vulnweb.com/listproducts.php?artist=1</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=2">http://testphp.vulnweb.com/listproducts.php?artist=2</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=3">http://testphp.vulnweb.com/listproducts.php?artist=3</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=1">http://testphp.vulnweb.com/listproducts.php?cat=1</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=2">http://testphp.vulnweb.com/listproducts.php?cat=2</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=3">http://testphp.vulnweb.com/listproducts.php?cat=3</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=4">http://testphp.vulnweb.com/listproducts.php?cat=4</a>
Method	GET
Parameter	

Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/login.php">http://testphp.vulnweb.com/login.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/product.php?pic=1">http://testphp.vulnweb.com/product.php?pic=1</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/product.php?pic=2">http://testphp.vulnweb.com/product.php?pic=2</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/product.php?pic=3">http://testphp.vulnweb.com/product.php?pic=3</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/product.php?pic=4">http://testphp.vulnweb.com/product.php?pic=4</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>

Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	POST
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Method	POST
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/secured/newuser.php">http://testphp.vulnweb.com/secured/newuser.php</a>
Method	POST
Parameter	
Attack	
Evidence	

Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-1] do not match.
Instances	31
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	<a href="https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection">https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection</a>
CWE Id	<a href="#">436</a>
WASC Id	15
Plugin Id	<a href="#">90011</a>

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	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	submit
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: <a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a> appears to include user input in: a(n) [input] tag [value] attribute The user input found was: submit=add message The user-controlled value was: add message
Request Header	POST http://testphp.vulnweb.com/guestbook.php HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache content-type: application/x-www-form-urlencoded referer: http://testphp.vulnweb.com/guestbook.php content-length: 33
Request Body	name=ZAP&text=&submit=add+message
Response Header	HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:13 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 5394
Response Body (truncated)	<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLOIsLocked="false" --> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">  <!-- InstanceBeginEditable name="document_title_rgn" --> <title>guestbook</title> <!-- InstanceEndEditable --> <link rel="stylesheet" href="style.css" type="text/css"> <!-- InstanceBeginEditable name="he...(truncated)
URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>

Method	POST
Parameter	goButton
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://testphp.vulnweb.com/search.php?test=query appears to include user input in: a(n) [input] tag [name] attribute The user input found was: goButton=go The user-controlled value was: gobutton
URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Method	POST
Parameter	goButton
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://testphp.vulnweb.com/search.php?test=query appears to include user input in: a(n) [input] tag [value] attribute The user input found was: goButton=go The user-controlled value was: go
Instances	3
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html</a>
CWE Id	<a href="#">20</a>
WASC Id	20
Plugin Id	<a href="#">10031</a>