

Site: http://testphp.vulnweb.com/

Generated on Sat, 11 May 2024 13:54:21

ZAP Version: 2.14.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	3
Informational	5
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	40
Content Security Policy (CSP) Header Not Set	Medium	48
Missing Anti-clickjacking Header	Medium	44
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	62
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	74
X-Content-Type-Options Header Missing	Low	68
Authentication Request Identified	Informational	1
<u>Charset Mismatch (Header Versus Meta Content-Type Charset)</u>	Informational	31
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	9
<u>User Controllable HTML Element Attribute</u> (<u>Potential XSS</u>)	Informational	3

Alert Detail

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

	user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.
Description	CSRF attacks are effective in a number of situations, including:
	* The victim has an active session on the target site.
	* The victim is authenticated via HTTP auth on the target site.
	* The victim is on the same local network as the target site.
	CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://testphp.vulnweb.com/
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/artists.php
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Evidence Other Info	<pre><form action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].</form></pre>
Other	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
Other Info URL	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. http://testphp.vulnweb.com/artists.php?artist=1
Other Info URL Method	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. http://testphp.vulnweb.com/artists.php?artist=1
Other Info URL Method Attack	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. http://testphp.vulnweb.com/artists.php?artist=1 GET
Other Info URL Method Attack Evidence Other	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. http://testphp.vulnweb.com/artists.php?artist=1 GET Cform action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following
Other Info URL Method Attack Evidence Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. http://testphp.vulnweb.com/artists.php?artist=1 GET Cform action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
Other Info URL Method Attack Evidence Other Info URL	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. http://testphp.vulnweb.com/artists.php?artist=1 GET Cform action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. http://testphp.vulnweb.com/artists.php?artist=2
Other Info URL Method Attack Evidence Other Info URL Method	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. http://testphp.vulnweb.com/artists.php?artist=1 GET Cform action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. http://testphp.vulnweb.com/artists.php?artist=2
Other Info URL Method Attack Evidence Other Info URL Method Attack	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, _csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. http://testphp.vulnweb.com/artists.php?artist=1 GET <pre></pre>
Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. http://testphp.vulnweb.com/artists.php?artist=1 GET <form action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, _csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. http://testphp.vulnweb.com/artists.php?artist=2 GET <form action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_token, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_magic, CSRF, _token, _csrf_token] was found in the following</form></form>
Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. http://testphp.vulnweb.com/artists.php?artist=1 GET <pre></pre>
Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL Method Attack URL URL URL URL URL URL URL UR	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. http://testphp.vulnweb.com/artists.php?artist=1 GET <pre> </pre> <pre> </pre> <pre> <pre> </pre> <pre> <pre></pre></pre></pre>

Evidence	<form action="search.php?test=query" method="post"></form>
	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken,
Other Info	csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/cart.php
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/categories.php
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Attack	
Evidence	<form action="" method="post" name="faddentry"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "name" "submit"].
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/index.php
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>

Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>

Other Info No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_tocsrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the folio HTML form: [Form 1: "goButton" "searchFor"]. URL http://testphp.vulnweb.com/listproducts.php?cat=4 Method GET Attack Evidence Attack Other Info Other Info Csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_tocsrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the folio HTML form: [Form 1: "goButton" "searchFor"]. URL http://testphp.vulnweb.com/login.php Method GET Attack Evidence <form action="userinfo.php" method="post" name="loginform"></form>	wing ken,
Method GET Attack Evidence <form action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_tocsrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the followable HTML form: [Form 1: "goButton" "searchFor"]. URL</form>	
Attack Evidence <form action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_tolen</form>	
Evidence <form action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_tocsrf,csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the followard form: [Form 1: "goButton" "searchFor"]. URL</form>	
No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_tocsrf,csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the follo HTML form: [Form 1: "goButton" "searchFor"]. URL	
Other csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_to lnfo csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the followaretoken that the local complete	
Method GET Attack	
Attack	
Evidence <form action="userinfo.php" method="post" name="loginform"></form>	
No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, Other csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_to Info csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the follo HTML form: [Form 1: "pass" "uname"].	
URL http://testphp.vulnweb.com/login.php	
Method GET	
Attack	
Evidence <form action="search.php?test=query" method="post"></form>	
No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_to Info	
URL http://testphp.vulnweb.com/product.php?pic=1	
Method GET	
Attack	
Evidence <form action="cart.php" method="POST" name="f_addcart"></form>	
No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_to Info	
URL http://testphp.vulnweb.com/product.php?pic=1	
Method GET	
Attack	
Evidence <form action="search.php?test=query" method="post"></form>	
<pre>Evidence</pre>	
Corm action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_to _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the followare token. Info	
<pre>Evidence</pre>	
Evidence <form action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_tocsrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the followard form: [Form 2: "goButton" "searchFor"]. URL</form>	

Other Info	csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "addcart" "price"].
URL	http://testphp.vulnweb.com/product.php?pic=2
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/product.php?pic=3
Method	GET
Attack	
Evidence	<form action="cart.php" method="POST" name="f_addcart"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "addcart" "price"].
URL	http://testphp.vulnweb.com/product.php?pic=3
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/product.php?pic=4
Method	GET
Attack	
Evidence	<form action="cart.php" method="POST" name="f_addcart"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "addcart" "price"].
URL	http://testphp.vulnweb.com/product.php?pic=4
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
Attack	
Evidence	<form action="cart.php" method="POST" name="f_addcart"></form>
Other	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token,

Info	_csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "addcart" "price"].
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Attack	
Evidence	<form action="cart.php" method="POST" name="f_addcart"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "addcart" "price"].
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Attack	
Evidence	<form action="cart.php" method="POST" name="f_addcart"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "addcart" "price"].
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Attack	
Evidence	<form action="/secured/newuser.php" method="post" name="form1"></form>
Other	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following

Info	HTML form: [Form 1: "signup" "ucc" "uemail" "upass" "upass2" "uphone" "urname" "uuname"].
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	
Evidence	<form action="" method="post" name="faddentry"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "name" "submit"].
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
Instances	40
	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).
Solution	Note that this can be bypassed using XSS.
	Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.
	Note that this can be bypassed using XSS.
	Use the ESAPI Session Management control.
	This control includes a component for CSRF.
	Do not use the GET method for any request that triggers a state change.
	Phase: Implementation
	Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross- Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	<u>352</u>
WASC Id	9
Plugin Id	10202
Plugin Id Medium	10202 Content Security Policy (CSP) Header Not Set
-	
Medium	Content Security Policy (CSP) Header Not Set 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
Medium Description	Content Security Policy (CSP) Header Not Set 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.
Medium Description URL	Content Security Policy (CSP) Header Not Set 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. http://testphp.vulnweb.com/
Medium Description URL Method	Content Security Policy (CSP) Header Not Set 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. http://testphp.vulnweb.com/
Medium Description URL Method Attack	Content Security Policy (CSP) Header Not Set 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. http://testphp.vulnweb.com/
Medium Description URL Method Attack Evidence Other	Content Security Policy (CSP) Header Not Set 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. http://testphp.vulnweb.com/
Medium Description URL Method Attack Evidence Other Info	Content Security Policy (CSP) Header Not Set 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. http://testphp.vulnweb.com/
Medium Description URL Method Attack Evidence Other Info URL	Content Security Policy (CSP) Header Not Set 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. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/index.php
Medium Description URL Method Attack Evidence Other Info URL Method	Content Security Policy (CSP) Header Not Set 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. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/index.php
Medium Description URL Method Attack Evidence Other Info URL Method Attack	Content Security Policy (CSP) Header Not Set 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. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/index.php
Medium Description URL Method Attack Evidence Other Info URL Method Attack Evidence Other Other	Content Security Policy (CSP) Header Not Set 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. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/index.php

Method

GET

Attack	
Evidence	
Other	
Info	
URL	http://testphp.vulnweb.com/artists.php?artist=1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/categories.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Attack	
Evidence	
Other Info	
	http://testphp.vulnweb.com/guestbook.php
Info	http://testphp.vulnweb.com/guestbook.php GET
Info URL	

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/?pp=12
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/index.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Attack	
Evidence	
Other	

Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/login.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/

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

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

Othor	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
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	https://developer.mozilla.org/en-US/docs/Web/Security/CSP /Introducing Content Security Policy https://cheatsheetseries.owasp.org/cheatsheets/Content Security Policy Cheat Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	<u>693</u>
CWE Id WASC Id	<u>693</u> 15
WASC Id	15
WASC Id Plugin Id	15 10038
WASC Id Plugin Id Medium	15 10038 Missing Anti-clickjacking Header The response does not include either Content-Security-Policy with 'frame-ancestors'
WASC Id Plugin Id Medium Description	15 10038 Missing Anti-clickjacking Header The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
WASC Id Plugin Id Medium Description URL	15 10038 Missing Anti-clickjacking Header The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks. http://testphp.vulnweb.com/
WASC Id Plugin Id Medium Description URL Method	15 10038 Missing Anti-clickjacking Header The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks. http://testphp.vulnweb.com/
WASC Id Plugin Id Medium Description URL Method Attack	15 10038 Missing Anti-clickjacking Header The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks. http://testphp.vulnweb.com/
WASC Id Plugin Id Medium Description URL Method Attack Evidence Other	15 10038 Missing Anti-clickjacking Header The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks. http://testphp.vulnweb.com/
WASC Id Plugin Id Medium Description URL Method Attack Evidence Other Info	15 10038 Missing Anti-clickjacking Header The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks. http://testphp.vulnweb.com/ GET
WASC Id Plugin Id Medium Description URL Method Attack Evidence Other Info URL	Missing Anti-clickjacking Header The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/index.php
WASC Id Plugin Id Medium Description URL Method Attack Evidence Other Info URL Method	Missing Anti-clickjacking Header The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/index.php
WASC Id Plugin Id Medium Description URL Method Attack Evidence Other Info URL Method Attack	Missing Anti-clickjacking Header The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/index.php
WASC Id Plugin Id Medium Description URL Method Attack Evidence Other Info URL Method Attack Evidence Other Other Info URL Method Attack Evidence Other	Missing Anti-clickjacking Header The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/index.php
WASC Id Plugin Id Medium Description URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info	Missing Anti-clickjacking Header The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/index.php GET
WASC Id Plugin Id Medium Description URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL Method Attack URL Method Attack URL Method Attack URL URL URL URL URL URL URL UR	Missing Anti-clickjacking Header The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/index.php GET http://testphp.vulnweb.com/AJAX/index.php

Other	
Info	http://tootahan.com/outists.ahanoartist.d
URL	http://testphp.vulnweb.com/artists.php?artist=1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/categories.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Attack	
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/hpp/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/?pp=12
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/index.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET

Attack	
Evidence	
Other	
Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/login.php
	OFT
Method	GET
Method Attack	GET
	GET
Attack	GET
Attack Evidence Other	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Attack Evidence Other Info	
Attack Evidence Other Info URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Attack Evidence Other Info URL Method	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Attack Evidence Other Info URL Method Attack	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Attack Evidence Other Info URL Method Attack Evidence Other	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Attack Evidence Other Info URL Method Attack Evidence Other Info	http://testphp.vulnweb.com/Mod_Rewrite_Shop/ GET
Attack Evidence Other Info URL Method Attack Evidence Other Info URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method	http://testphp.vulnweb.com/Mod_Rewrite_Shop/ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack	http://testphp.vulnweb.com/Mod_Rewrite_Shop/ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other	http://testphp.vulnweb.com/Mod_Rewrite_Shop/ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info	http://testphp.vulnweb.com/Mod_Rewrite_Shop/ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/ GET
Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence URL Method Attack Evidence URL Method Attack URL URL URL URL URL URL URL URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/

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

Info	
URL	http://testphp.vulnweb.com/product.php?pic=1
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=2
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=3
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=4
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/signup.php

Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
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	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020
Low	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

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

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

	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other	7. Tomorou By. This your to be rubuniu Both and should be rubuniu Both and
	Info 	
UI	RL	http://testphp.vulnweb.com/listproducts.php?artist=2
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
UI	RL	http://testphp.vulnweb.com/listproducts.php?artist=3
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
UI	RL	http://testphp.vulnweb.com/listproducts.php?cat=1
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
UI	RL	http://testphp.vulnweb.com/listproducts.php?cat=2
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
UI	RL	http://testphp.vulnweb.com/listproducts.php?cat=3
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
UI	RL	http://testphp.vulnweb.com/listproducts.php?cat=4
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
UI	RL	http://testphp.vulnweb.com/login.php
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other	

Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other	
Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html

Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other	7. 1 chiefe 2 27. 1 11 / cles 10 ce 1 azantazete 11 1 acz. ca. 1 1 cig. 1
Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/privacy.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=1
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=2
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=3
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=4
Method	GET

Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other	At one of Eyr, the foliation of the analysis and the grant of the gran
Info	
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
Method	GET
Attack	

Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&size=160
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other	

Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&size=160
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php

Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
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	https://owasp.org/www-project-web-security-testing-guide/v42/4- Web Application Security Testing/01-Information Gathering/08- Fingerprint Web Application Framework https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	200
WASC Id	13
Plugin Id	10037
Low	Server Leaks Version Information via "Server" HTTP Response Header Field
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	http://testphp.vulnweb.com/
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET

Out	
Other Info	
URL	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Flash/add.swf
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/high
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/hpp/
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/hpp/?pp=12
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	

URL	http://testphp.vulnweb.com/images/logo.gif
Method	GET
Attack	
Evidence	nginx/1.19.0
Other	
Info	
URL	http://testphp.vulnweb.com/images/remark.gif
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/index.php
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET

Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=3
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/login.php
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Method	GET
Attack	

Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Method	GET
Attack	
Evidence	nginx/1.19.0
Other	

Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Method	GET
Attack	
Evidence	nginx/1.19.0
Other	
Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/privacy.php
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=1
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=2
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=3
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=4
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=5

8.6 (1)	OFT
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/secured/style.css
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
Method	GET

Attack	
Evidence	nginx/1.19.0
Other	
Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
Method	GET
Attack	
Evidence	nginx/1.19.0
Other	
Info	
Info URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160 GET
URL	
URL Method	
URL Method Attack	GET
URL Method Attack Evidence Other	GET
URL Method Attack Evidence Other Info	GET nginx/1.19.0
URL Method Attack Evidence Other Info URL	GET nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
URL Method Attack Evidence Other Info URL Method	GET nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
URL Method Attack Evidence Other Info URL Method Attack	GET nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg GET
URL Method Attack Evidence Other Info URL Method Attack Evidence Other	GET nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg GET
URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info	nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg GET nginx/1.19.0
URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL URL URL Method Attack URL URL URL URL URL URL	nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg GET nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Method Attack Evidence Other Info URL Method	GET nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg GET nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Attack	nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg GET nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160 GET
URL Method Attack Evidence Other Info URL	nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg GET nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160 GET
URL Method Attack Evidence Other Info	nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg GET nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160 GET nginx/1.19.0
URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL Method Attack URL Method Attack URL Method Attack URL URL URL URL URL URL URL UR	nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg GET nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160 GET nginx/1.19.0 http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg

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

URL	http://testphp.vulnweb.com/style.css
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Attack	
Evidence	nginx/1.19.0
Other Info	
Instances	74

Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	<u>200</u>
WASC Id	13
Plugin Id	<u>10036</u>
Low	V Content Type Ontions Header Missing
Description	X-Content-Type-Options Header Missing The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://testphp.vulnweb.com/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/styles.css
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/artists.php
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/artists.php?artist=1
Method	GET

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/artists.php?artist=2
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/cart.php
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/categories.php
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/disclaimer.php
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Flash/add.swf
Method	GET
Attack	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/hpp/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/hpp/?pp=12
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/images/logo.gif
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/images/remark.gif
Method	GET
Attack	

F	Evidence	
_		This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still
	Other nfo	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	-	http://testphp.vulnweb.com/index.php
N	Method	GET
Α	Attack	
E	Evidence	
	Other nfo	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	-	http://testphp.vulnweb.com/listproducts.php?artist=1
N	Method	GET
Д	Attack	
Е	Evidence	
_	Other nfo	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	-	http://testphp.vulnweb.com/listproducts.php?artist=2
N	Method	GET
Δ	Attack	
Е	Evidence	
	Other nfo	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	-	http://testphp.vulnweb.com/listproducts.php?artist=3
N	Method	GET
Α	Attack	
Е	Evidence	
	Other nfo	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	-	http://testphp.vulnweb.com/listproducts.php?cat=1
N	Method	GET
Д	Attack	
E	Evidence	
	Other nfo	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	_	http://testphp.vulnweb.com/listproducts.php?cat=2
N	Method	GET
Δ	Attack	
Е	Evidence	

	Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
UF	RL	http://testphp.vulnweb.com/listproducts.php?cat=3
	Method	GET
	Attack	
	Evidence	
	Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
UF	RL	http://testphp.vulnweb.com/listproducts.php?cat=4
	Method	GET
	Attack	
	Evidence	
	Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
UF	RL	http://testphp.vulnweb.com/login.php
	Method	GET
	Attack	
	Evidence	
	Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
UF	RL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
	Method	GET
	Attack	
	Evidence	
	Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
UF	₹L	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
	Method	GET
	Attack	
	Evidence	
	Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
UF	RL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
	Method	GET
	Attack	
	Evidence	

	This issue still applies to error type pages (401, 402, 500, etc.) as these pages are after atill
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg
Method	GET
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Other Info	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/product.php?pic=1
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/product.php?pic=2
Method	GET
Attack	
Evidence	
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/product.php?pic=3
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/product.php?pic=4
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/secured/style.css
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client

	or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client

	or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
Method	GET
Attack	OET .
Evidence	
Evidence	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still
Other Info	affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&size=160
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

Wethod GET Attack Evidence Other Info GET Attack Evidence Other Info GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/showimage.php?file=/pictures/7.jpg Method GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/showimage.php?file=/pictures/7.jpg&sizze=160 Other Info GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/signup.php Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/signup.php GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.ess This issue still applies to error type pages	URL	
Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/showimage.php?file=/pictures/7.jpg Method GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/showimage.php?file=/pictures/7.jpg&size=160 Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/signup.php Method GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) a		http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/showimage.php?file=/pictures/7.jpg Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/showimage.php?file=/pictures/7.jpg&size=160 GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/signup.php Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/siyle.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/siyle.css This issue still applies to error type pages (401, 403, 500, etc.) as those p	Method	GET
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers snifting pages away from their actual content type. At 'High' threshold this scan rule will not alert on client or server error responses. URL Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers snifting pages away from their actual content type. At 'High' threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/showimage.php?file=/pictures/7.jpg&size=160 Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At 'High' threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/signup.php Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still other affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At 'High' threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/signup.php Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At 'High' threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/signup.php Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by in	Attack	
Other Info area yrom their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/showimage.php?file=/pictures/7.jpg Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/showimage.php?file=/pictures/7.jpg&size=160 GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/signup.php Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection	Evidence	
Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/showimage.php?file=/pictures/7.jpg&size=160 Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/signup.php Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php This issue still applies to error type pages (401, 403, 500, etc.)		affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client
Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not allert on client or server error responses. URL Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not allert on client or server error responses. URL Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not allert on client or server error responses. URL Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not allert on client or server error responses. URL Method GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages and for away from their actual content type. At "High" threshold this scan rule will not allert on client or server error responses. URL Method POST This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by	URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg
Cither Info Other Info Info Other Info Info Other Info Other Info Info Other	Method	GET
Other Info	Attack	
Other Info away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/showimage.php?file=/pictures/7.jpg&size=160 Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/signup.php GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages in for the way from their actual content type. At "High" thres	Evidence	
Method Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/signup.php Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are way from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still on server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the page and the page are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their act		affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client
Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/signup.php GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.	URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&size=160
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/signup.php Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client	Method	GET
Other Info	Attack	
Other Info affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/signup.php Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the page and the page a	Evidence	
Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still on the case there is still concern for browsers sniffing pages are often still on the case there is still concern for browsers sniffing pages are often still on the case there is still concern for browsers sniffing pages are often still on the case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the case there is still concern for browsers sniffing pages away from their actual content type.		affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client
Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client	URL	http://testphp.vulnweb.com/signup.php
Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client	Method	GET
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client	Attack	
Other Info affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/style.css Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the saway from their actual content type. At "High" threshold this scan rule will not alert on client	Evidence	
Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client		
Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client		away from their actual content type. At "High" threshold this scan rule will not alert on client
Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client	Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Other Info Other Info Other Info Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client	Info URL	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/style.css
Other Info adjected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/cart.php Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client	Info URL Method	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/style.css
Method POST Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client	Info URL Method Attack	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/style.css
Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages lnfo away from their actual content type. At "High" threshold this scan rule will not alert on client	Info URL Method Attack Evidence Other	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/style.css GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client
Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client	Info URL Method Attack Evidence Other Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/style.css GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client	Info URL Method Attack Evidence Other Info URL	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/style.css GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/cart.php
Other affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client	Info URL Method Attack Evidence Other Info URL Method	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/style.css GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/cart.php
	Info URL Method Attack Evidence Other Info URL Method Attack	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/style.css GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/cart.php

URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	60
Instances	68
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.
	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
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. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)
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. https://earn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) <a compatibility="" en-us="" gg622941(v='vs.85)"' href="https://example.com/https://ex</td></tr><tr><td>Solution Reference CWE Id</td><td>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. https://explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security-Headers
Solution Reference CWE Id WASC Id Plugin Id	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. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers 693 15 10021
Solution Reference CWE Id WASC Id	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. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers 693 15
Solution Reference CWE Id WASC Id Plugin Id Informational	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. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers 693 15 10021 Authentication Request Identified 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
Solution Reference CWE Id WASC Id Plugin Id Informational Description	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. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer /compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers 693 15 10021 Authentication Request Identified 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.
Solution Reference CWE Id WASC Id Plugin Id Informational Description URL	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. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer /compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers 693 15 10021 Authentication Request Identified 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. http://testphp.vulnweb.com/secured/newuser.php
Solution Reference CWE Id WASC Id Plugin Id Informational Description URL Method	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. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer /compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers 693 15 10021 Authentication Request Identified 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. http://testphp.vulnweb.com/secured/newuser.php POST
Solution Reference CWE Id WASC Id Plugin Id Informational Description URL Method Attack Evidence Other	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. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer /compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers 693 15 10021 Authentication Request Identified 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. http://testphp.vulnweb.com/secured/newuser.php POST upass userParam=uemail userValue=ZAP passwordParam=upass referer=http://testphp.vulnweb.
Solution Reference CWE Id WASC Id Plugin Id Informational Description URL Method Attack Evidence	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-sniifting at all, or that can be directed by the web application /web server to not perform MIME-sniifting. https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer /compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers 693 15 10021 Authentication Request Identified 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. http://testphp.vulnweb.com/secured/newuser.php POST

Reference https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/ CWE Id WASC Id	Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
WASC Id	Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
	CWE Id	
	WASC Id	
Plugin Id <u>10111</u>	Plugin Id	<u>10111</u>

VVAOO IU	
Plugin Id	<u>10111</u>
Informational	Charset Mismatch (Header Versus Meta Content-Type Charset)
Description	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set. An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.
URL	http://testphp.vulnweb.com/
Method	GET
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	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
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	http://testphp.vulnweb.com/artists.php
Method	GET
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	http://testphp.vulnweb.com/artists.php?artist=1
Method	GET
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	http://testphp.vulnweb.com/artists.php?artist=2
Method	GET
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	http://testphp.vulnweb.com/artists.php?artist=3

Method	GET
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	http://testphp.vulnweb.com/cart.php
Method	GET
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	http://testphp.vulnweb.com/categories.php
Method	GET
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	http://testphp.vulnweb.com/disclaimer.php
Method	GET
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	http://testphp.vulnweb.com/guestbook.php
Method	GET
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	http://testphp.vulnweb.com/index.php
Method	GET
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	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET
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	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Attack	

Evidence	
Other	There was a charset mismatch between the HTTP Header and the META content-type
Info	encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	http://testphp.vulnweb.com/listproducts.php?artist=3
Method	GET
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	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET
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	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET
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	http://testphp.vulnweb.com/listproducts.php?cat=3
Method	GET
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	http://testphp.vulnweb.com/listproducts.php?cat=4
Method	GET
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	http://testphp.vulnweb.com/login.php
Method	GET
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	http://testphp.vulnweb.com/product.php?pic=1
Method	GET
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	http://testphp.vulnweb.com/product.php?pic=2
Method	GET
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	http://testphp.vulnweb.com/product.php?pic=3
Method	GET
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	http://testphp.vulnweb.com/product.php?pic=4
Method	GET
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	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
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	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
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	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
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	http://testphp.vulnweb.com/signup.php
Method	GET
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	http://testphp.vulnweb.com/cart.php
Method	POST
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	http://testphp.vulnweb.com/guestbook.php
Method	POST
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	http://testphp.vulnweb.com/search.php?test=query
Method	POST
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	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
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	https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id	436
WASC Id	15
Plugin Id	90011
Informational	Information Disclosure - Suspicious Comments

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected in the element starting with: " <script type="text/javascript"> var httpreq = null; function SetContent(XML) { var items = XML.getElementsByTagName('i", see evidence field for the suspicious comment/snippet.</td></tr><tr><td>Instances</td><td>1</td></tr><tr><td>Solution</td><td>Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.</td></tr><tr><td>Reference</td><td></td></tr></tbody></table></script>

CWE Id	<u>200</u>
WASC Id	13
Plugin Id	<u>10027</u>

Informational	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
Attack	
Evidence	titles
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/artists.php
Method	GET
Attack	
Evidence	comment on this artist
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/artists.php?artist=1
Method	GET
Attack	
Evidence	comment on this artist
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/artists.php?artist=2
Method	GET
Attack	
Evidence	comment on this artist
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET
Attack	
Evidence	comment on this artist
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET
Attack	
Evidence	comment on this picture

Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Attack	
Evidence	comment on this picture
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET
Attack	
Evidence	comment on this picture
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET
Attack	
Evidence	comment on this picture
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Instances	9
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	<u>10109</u>
Informational	User Controllable HTML Element Attribute (Potential XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://testphp.vulnweb.com/guestbook.php 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
URL	http://testphp.vulnweb.com/search.php?test=query
URL Method	
	http://testphp.vulnweb.com/search.php?test=query
Method	http://testphp.vulnweb.com/search.php?test=query
Method Attack	http://testphp.vulnweb.com/search.php?test=query

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	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://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	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	<u>20</u>
WASC Id	20
Plugin Id	10031