

# VirtuesTech Security Scan Report

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

Generated on Mon, 7 Apr 2025 18:54:26

## Summary of Alerts

RISK LEVEL	NUMBER OF ALERTS
High	0
Medium	3
Low	3
Informational	4
False Positives:	0

## Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

## Alerts

NAME	RISK LEVEL	NUMBER OF INSTANCES
<a href="#">Absence of Anti-CSRF Tokens</a>	Medium	40
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	48
<a href="#">Missing Anti-clickjacking Header</a>	Medium	44
<a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</a>	Low	62
<a href="#">Server Leaks Version Information via "Server" HTTP Response Header Field</a>	Low	74
<a href="#">X-Content-Type-Options Header Missing</a>	Low	68
<a href="#">Authentication Request Identified</a>	Informational	1
<a href="#">Charset Mismatch (Header Versus Meta Content-Type Charset)</a>	Informational	31

[Modern Web Application](#)

Informational

9

[User Controllable HTML Element Attribute \(Potential XSS\)](#)

Informational

3

## Alert Detail

MEDIUM	ABSENCE OF ANTI-CSRF TOKENS
Description	<p>No Anti-CSRF tokens were found in a HTML submission form.</p> <p>A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.</p> <p>CSRF attacks are effective in a number of situations, including:</p> <ul style="list-style-type: none"><li>* The victim has an active session on the target site.</li><li>* The victim is authenticated via HTTP auth on the target site.</li><li>* The victim is on the same local network as the target site.</li></ul> <p>CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.</p>
URL	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">

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

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

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

Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=2">http://testphp.vulnweb.com/listproducts.php?cat=2</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=3">http://testphp.vulnweb.com/listproducts.php?cat=3</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/listproducts.php?cat=4">http://testphp.vulnweb.com/listproducts.php?cat=4</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/login.php">http://testphp.vulnweb.com/login.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form name="loginform" method="post" action="userinfo.php">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "pass" "uname" ].

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

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



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

URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	
Attack	
Evidence	<form name='f_addcart' method='POST' action='cart.php'>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "addcart" "price" ].
URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 2: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form name="form1" method="post" action="/secured/newuser.php">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "signup" "ucc" "uemail" "upass" "upass2" "uphone" "urname" "uuname" ].
URL	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 2: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	POST

Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF_token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	
Attack	
Evidence	<form action="" method="post" name="faddentry">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF_token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "name" "submit" ].
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF_token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 2: "goButton" "searchFor" ].
URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Method	POST
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF_token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "goButton" "searchFor" ].
Instances	40

Solution	Phase: Architecture and Design
	Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
	For example, use anti-CSRF packages such as the OWASP CSRFGuard.
	Phase: Implementation
	Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.
	Phase: Architecture and Design
	Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).
	Note that this can be bypassed using XSS.
	Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.
	Note that this can be bypassed using XSS.
	Use the ESAPI Session Management control.
	This control includes a component for CSRF.
	Do not use the GET method for any request that triggers a state change.
	Phase: Implementation
	Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html</a> <a href="https://cwe.mitre.org/data/definitions/352.html">https://cwe.mitre.org/data/definitions/352.html</a>
CWE Id	<a href="#">352</a>
WASC Id	9
Plugin Id	<a href="#">10202</a>

MEDIUM	CONTENT SECURITY POLICY (CSP) HEADER NOT SET
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>

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

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

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

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



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

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

Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=3">http://testphp.vulnweb.com/product.php?pic=3</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=4">http://testphp.vulnweb.com/product.php?pic=4</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/robots.txt">http://testphp.vulnweb.com/robots.txt</a>

Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/sitemap.xml">http://testphp.vulnweb.com/sitemap.xml</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Method	POST
Parameter	
Attack	
Evidence	

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

<b>MEDIUM</b>	<b>MISSING ANTI-CLICKJACKING HEADER</b>
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/AJAX/index.php">http://testphp.vulnweb.com/AJAX/index.php</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	

Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=1">http://testphp.vulnweb.com/artists.php?artist=1</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=2">http://testphp.vulnweb.com/artists.php?artist=2</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=3">http://testphp.vulnweb.com/artists.php?artist=3</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/categories.php">http://testphp.vulnweb.com/categories.php</a>
Method	GET

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

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



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

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

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

Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=4">http://testphp.vulnweb.com/product.php?pic=4</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	POST

Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	<a href="http://testphp.vulnweb.com/secured/newuser.php">http://testphp.vulnweb.com/secured/newuser.php</a>
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
Instances	44
Solution	<p>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.</p> <p>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.</p>
Reference	<a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a>
CWE Id	<a href="#">1021</a>
WASC Id	15
Plugin Id	<a href="#">10020</a>

LOW

SERVER LEAKS INFORMATION VIA "X-POWERED-BY" HTTP RESPONSE HEADER FIELD(S)

Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/AJAX/index.php">http://testphp.vulnweb.com/AJAX/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=1">http://testphp.vulnweb.com/artists.php?artist=1</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=2">http://testphp.vulnweb.com/artists.php?artist=2</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	

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

Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/hpp/?pp=12">http://testphp.vulnweb.com/hpp/?pp=12</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/hpp/params.php?p=valid&amp;pp=12">http://testphp.vulnweb.com/hpp/params.php?p=valid&amp;pp=12</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/index.php">http://testphp.vulnweb.com/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=1">http://testphp.vulnweb.com/listproducts.php?artist=1</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=2">http://testphp.vulnweb.com/listproducts.php?artist=2</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	



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

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

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

Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=1">http://testphp.vulnweb.com/product.php?pic=1</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=2">http://testphp.vulnweb.com/product.php?pic=2</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=3">http://testphp.vulnweb.com/product.php?pic=3</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=4">http://testphp.vulnweb.com/product.php?pic=4</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'">http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg</a>
Method	GET

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

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

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



Other Info	
URL	<a href="http://testphp.vulnweb.com/secured/newuser.php">http://testphp.vulnweb.com/secured/newuser.php</a>
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	<a href="http://testphp.vulnweb.com/userinfo.php">http://testphp.vulnweb.com/userinfo.php</a>
Method	POST
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
Instances	62
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	<a href="https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework">https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework</a> <a href="https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html">https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html</a>
CWE Id	<a href="#">497</a>
WASC Id	13
Plugin Id	<a href="#">10037</a>

LOW	SERVER LEAKS VERSION INFORMATION VIA "SERVER" HTTP RESPONSE HEADER FIELD
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	

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

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

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

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

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

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

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



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

Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/robots.txt">http://testphp.vulnweb.com/robots.txt</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/secured/style.css">http://testphp.vulnweb.com/secured/style.css</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'">http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'</a>
Method	GET

Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0

Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&amp;size=160</a>
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg</a>
Method	GET

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

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

Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	<a href="http://testphp.vulnweb.com/userinfo.php">http://testphp.vulnweb.com/userinfo.php</a>
Method	POST
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
Instances	74
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	<a href="https://httpd.apache.org/docs/current/mod/core.html#servertokens">https://httpd.apache.org/docs/current/mod/core.html#servertokens</a> <a href="https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)">https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)</a> <a href="https://www.troyhunt.com/shhh-dont-let-your-response-headers/">https://www.troyhunt.com/shhh-dont-let-your-response-headers/</a>
CWE Id	<a href="#">497</a>
WASC Id	13
Plugin Id	<a href="#">10036</a>

<b>LOW</b>	<b>X-CONTENT-TYPE-OPTIONS HEADER MISSING</b>
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/AJAX/index.php">http://testphp.vulnweb.com/AJAX/index.php</a>

Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/AJAX/styles.css">http://testphp.vulnweb.com/AJAX/styles.css</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=1">http://testphp.vulnweb.com/artists.php?artist=1</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/artists.php?artist=2">http://testphp.vulnweb.com/artists.php?artist=2</a>
Method	GET
Parameter	x-content-type-options
Attack	



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

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

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/images/logo.gif">http://testphp.vulnweb.com/images/logo.gif</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/images/remark.gif">http://testphp.vulnweb.com/images/remark.gif</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/index.php">http://testphp.vulnweb.com/index.php</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/listproducts.php?artist=1">http://testphp.vulnweb.com/listproducts.php?artist=1</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	

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

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

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

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

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



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

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/secured/style.css">http://testphp.vulnweb.com/secured/style.css</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'">http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

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

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

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&amp;size=160</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg">http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&amp;size=160">http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&amp;size=160</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/style.css">http://testphp.vulnweb.com/style.css</a>
Method	GET
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Method	POST

Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://testphp.vulnweb.com/secured/newuser.php">http://testphp.vulnweb.com/secured/newuser.php</a>
Method	POST
Parameter	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	68
Solution	<p>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.</p> <p>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.</p>
Reference	<a href="https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)">https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)</a> <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10021</a>

INFORMATIONAL	AUTHENTICATION REQUEST IDENTIFIED
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	<a href="http://testphp.vulnweb.com/secured/newuser.php">http://testphp.vulnweb.com/secured/newuser.php</a>
Method	POST
Parameter	uemail
Attack	

Evidence	upass
Other Info	userParam=uemail userValue=ZAP passwordParam=upass referer=http://testphp.vulnweb.com/signup.php
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	<a href="https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/">https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10111</a>

INFORMATIONAL	CHARSET MISMATCH (HEADER VERSUS META CONTENT-TYPE CHARSET)
Description	<p>This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set.</p> <p>An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.</p>
URL	<a href="http://testphp.vulnweb.com/">http://testphp.vulnweb.com/</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/AJAX/index.php">http://testphp.vulnweb.com/AJAX/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-1] do not match.
URL	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Method	GET
Parameter	



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

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

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

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

Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/product.php?pic=5">http://testphp.vulnweb.com/product.php?pic=5</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/product.php?pic=6">http://testphp.vulnweb.com/product.php?pic=6</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/product.php?pic=7">http://testphp.vulnweb.com/product.php?pic=7</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/signup.php">http://testphp.vulnweb.com/signup.php</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/cart.php">http://testphp.vulnweb.com/cart.php</a>
Method	POST
Parameter	

Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Method	POST
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	<a href="http://testphp.vulnweb.com/secured/newuser.php">http://testphp.vulnweb.com/secured/newuser.php</a>
Method	POST
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-1] do not match.
Instances	31
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	<a href="https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection">https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection</a>
CWE Id	<a href="#">436</a>
WASC Id	15
Plugin Id	<a href="#">90011</a>

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	<a href="http://testphp.vulnweb.com/AJAX/index.php">http://testphp.vulnweb.com/AJAX/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	<a href="#" onclick="loadSomething('titles.php')">titles</a>
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	<a href="http://testphp.vulnweb.com/artists.php">http://testphp.vulnweb.com/artists.php</a>
Method	GET
Parameter	
Attack	
Evidence	<a href="#" onClick="window.open('./comment.php?aid=1','comment','width=500,height=400')">comment on this artist</a>
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	<a href="http://testphp.vulnweb.com/artists.php?artist=1">http://testphp.vulnweb.com/artists.php?artist=1</a>
Method	GET
Parameter	
Attack	
Evidence	<a href="#" onClick="window.open('./comment.php?aid=1','comment','width=500,height=400')">comment on this artist</a>
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	<a href="http://testphp.vulnweb.com/artists.php?artist=2">http://testphp.vulnweb.com/artists.php?artist=2</a>
Method	GET
Parameter	
Attack	
Evidence	<a href="#" onClick="window.open('./comment.php?aid=2','comment','width=500,height=400')">comment on this artist</a>
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	<a href="http://testphp.vulnweb.com/artists.php?artist=3">http://testphp.vulnweb.com/artists.php?artist=3</a>

Method	GET
Parameter	
Attack	
Evidence	<a href='#' onClick="window.open('./comment.php?aid=3','comment','width=500,height=400')">comment on this artist</a>
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	<a href="http://testphp.vulnweb.com/listproducts.php?artist=1">http://testphp.vulnweb.com/listproducts.php?artist=1</a>
Method	GET
Parameter	
Attack	
Evidence	<a href='#' onClick="window.open('./comment.php?pid=1','comment','width=500,height=400')">comment on this picture</a>
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	<a href="http://testphp.vulnweb.com/listproducts.php?artist=2">http://testphp.vulnweb.com/listproducts.php?artist=2</a>
Method	GET
Parameter	
Attack	
Evidence	<a href='#' onClick="window.open('./comment.php?pid=7','comment','width=500,height=400')">comment on this picture</a>
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	<a href="http://testphp.vulnweb.com/listproducts.php?cat=1">http://testphp.vulnweb.com/listproducts.php?cat=1</a>
Method	GET
Parameter	
Attack	
Evidence	<a href='#' onClick="window.open('./comment.php?pid=1','comment','width=500,height=400')">comment on this picture</a>
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	<a href="http://testphp.vulnweb.com/listproducts.php?cat=2">http://testphp.vulnweb.com/listproducts.php?cat=2</a>
Method	GET
Parameter	



Attack	
Evidence	<a href='#' onClick="window.open('./comment.php?pid=6','comment','width=500,height=400')">comment on this picture</a>
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	<a href="#">10109</a>

INFORMATIONAL	USER CONTROLLABLE HTML ELEMENT ATTRIBUTE (POTENTIAL XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	<a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a>
Method	POST
Parameter	submit
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: <a href="http://testphp.vulnweb.com/guestbook.php">http://testphp.vulnweb.com/guestbook.php</a> appears to include user input in: a(n) [input] tag [value] attribute The user input found was: submit=add message The user-controlled value was: add message
URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Method	POST
Parameter	goButton
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: <a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a> appears to include user input in: a(n) [input] tag [name] attribute The user input found was: goButton=go The user-controlled value was: gobutton

URL	<a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a>
Method	POST
Parameter	goButton
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: <a href="http://testphp.vulnweb.com/search.php?test=query">http://testphp.vulnweb.com/search.php?test=query</a> appears to include user input in: a(n) [input] tag [value] attribute The user input found was: goButton=go The user-controlled value was: go
Instances	3
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html</a>
CWE Id	<a href="#">20</a>
WASC Id	20
Plugin Id	<a href="#">10031</a>

## Sequence Details

With the associated active scan results.

Report generated by VirtuesTech Security Scanner

