



**Sites:** <http://testphp.vulnweb.com> <https://thethrone.in>

**Generated on Thu, 17 Apr 2025 19:27:51**

### Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	7
Low	9
Informational	8
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	42
<a href="#">CSP: Failure to Define Directive with No Fallback</a>	Medium	1
<a href="#">CSP: Wildcard Directive</a>	Medium	1
<a href="#">CSP: script-src unsafe-inline</a>	Medium	1
<a href="#">CSP: style-src unsafe-inline</a>	Medium	1
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	54
<a href="#">Missing Anti-clickjacking Header</a>	Medium	44
<a href="#">Cookie No HttpOnly Flag</a>	Low	4
<a href="#">Cookie Without Secure Flag</a>	Low	6
<a href="#">Cookie without SameSite Attribute</a>	Low	1
<a href="#">Cross-Domain JavaScript Source File Inclusion</a>	Low	2
<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="#">Strict-Transport-Security Header Not Set</a>	Low	8
<a href="#">Timestamp Disclosure - Unix</a>	Low	15
<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
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	1
<a href="#">Modern Web Application</a>	Informational	10
<a href="#">Re-examine Cache-control Directives</a>	Informational	1
<a href="#">Retrieved from Cache</a>	Informational	1
<a href="#">Session Management Response Identified</a>	Informational	1
<a href="#">User Controllable HTML Element Attribute (Potential XSS)</a>	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" "uname" "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="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	<form action="/cart" id="CartDrawer-Form" class="cart__contents cart-drawer__form" 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: "" ].
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>

Method	GET
Parameter	
Attack	
Evidence	<form method="post" action="/contact#ContactFooter" id="ContactFooter" accept-charset="UTF-8" class="footer__newsletter newsletter-form">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 3: "contact[tags]" "form_type" "NewsletterForm--sections--23415186129206__footer" "utf8" ].
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	42
Solution	<p>Phase: Architecture and Design</p> <p>Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.</p> <p>For example, use anti-CSRF packages such as the OWASP CSRFGuard.</p> <p>Phase: Implementation</p> <p>Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.</p> <p>Phase: Architecture and Design</p> <p>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).</p> <p>Note that this can be bypassed using XSS.</p> <p>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.</p> <p>Note that this can be bypassed using XSS.</p> <p>Use the ESAPI Session Management control.</p> <p>This control includes a component for CSRF.</p> <p>Do not use the GET method for any request that triggers a state change.</p> <p>Phase: Implementation</p>

	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>

<b>Medium</b>	<b>CSP: Failure to Define Directive with No Fallback</b>
Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing/excluding them is the same as allowing anything.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	content-security-policy
Attack	
Evidence	block-all-mixed-content; frame-ancestors 'none'; upgrade-insecure-requests;
Other Info	The directive(s): form-action is/are among the directives that do not fallback to default-src.
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	<a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://caniuse.com/#search=content+security+policy">https://caniuse.com/#search=content+security+policy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a> <a href="https://github.com/HtmlUnit/htmlunit-csp">https://github.com/HtmlUnit/htmlunit-csp</a> <a href="https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources">https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10055</a>



Medium	CSP: Wildcard Directive
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	content-security-policy
Attack	
Evidence	block-all-mixed-content; frame-ancestors 'none'; upgrade-insecure-requests;
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	<a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://caniuse.com/#search=content+security+policy">https://caniuse.com/#search=content+security+policy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a> <a href="https://github.com/HtmlUnit/htmlunit-csp">https://github.com/HtmlUnit/htmlunit-csp</a> <a href="https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources">https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10055</a>

Medium	CSP: script-src unsafe-inline
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	content-security-policy
Attack	
Evidence	block-all-mixed-content; frame-ancestors 'none'; upgrade-insecure-requests;
Other Info	script-src includes unsafe-inline.
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	<a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://caniuse.com/#search=content+security+policy">https://caniuse.com/#search=content+security+policy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a> <a href="https://github.com/HtmlUnit/htmlunit-csp">https://github.com/HtmlUnit/htmlunit-csp</a> <a href="https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources">https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10055</a>

Medium	CSP: style-src unsafe-inline
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	content-security-policy
Attack	
Evidence	block-all-mixed-content; frame-ancestors 'none'; upgrade-insecure-requests;
Other Info	style-src includes unsafe-inline.
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	<a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://caniuse.com/#search=content+security+policy">https://caniuse.com/#search=content+security+policy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a> <a href="https://github.com/HtmlUnit/htmlunit-csp">https://github.com/HtmlUnit/htmlunit-csp</a> <a href="https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources">https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10055</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="https://thethrone.in">https://thethrone.in</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://thethrone.in/cdn-cgi">https://thethrone.in/cdn-cgi</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://thethrone.in/cdn-cgi/styles">https://thethrone.in/cdn-cgi/styles</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://thethrone.in/robots.txt">https://thethrone.in/robots.txt</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://thethrone.in/sitemap.xml">https://thethrone.in/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	54
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>

Medium	Missing Anti-clickjacking Header
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	<a href="http://testphp.vulnweb.com">http://testphp.vulnweb.com</a>
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
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	Cookie No HttpOnly Flag
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	_shopify_s
Attack	
Evidence	set-cookie: _shopify_s
Other Info	
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	_shopify_y
Attack	
Evidence	set-cookie: _shopify_y
Other Info	
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	_tracking_consent
Attack	
Evidence	set-cookie: _tracking_consent
Other Info	
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	localization
Attack	
Evidence	set-cookie: localization
Other Info	
Instances	4
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	<a href="https://owasp.org/www-community/HttpOnly">https://owasp.org/www-community/HttpOnly</a>
CWE Id	<a href="#">1004</a>
WASC Id	13



Plugin Id	<a href="#">10010</a>
-----------	-----------------------

Low	Cookie Without Secure Flag
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	_landing_page
Attack	
Evidence	set-cookie: _landing_page
Other Info	
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	_orig_referrer
Attack	
Evidence	set-cookie: _orig_referrer
Other Info	
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	_shopify_s
Attack	
Evidence	set-cookie: _shopify_s
Other Info	
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	_shopify_y
Attack	
Evidence	set-cookie: _shopify_y
Other Info	
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	_tracking_consent
Attack	
Evidence	set-cookie: _tracking_consent
Other Info	

URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	localization
Attack	
Evidence	set-cookie: localization
Other Info	
Instances	6
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	<a href="https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html">https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html</a>
CWE Id	<a href="#">614</a>
WASC Id	13
Plugin Id	<a href="#">10011</a>

<b>Low</b>	<b>Cookie without SameSite Attribute</b>
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	localization
Attack	
Evidence	set-cookie: localization
Other Info	
Instances	1
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	<a href="https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site">https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site</a>
CWE Id	<a href="#">1275</a>
WASC Id	13
Plugin Id	<a href="#">10054</a>

Low	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	https://unpkg.com/@google/model-viewer/dist/model-viewer-legacy.js
Attack	
Evidence	<script nomodule src="https://unpkg.com/@google/model-viewer/dist/model-viewer-legacy.js"></script>
Other Info	
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	https://unpkg.com/@google/model-viewer/dist/model-viewer.js
Attack	
Evidence	<script type="module" src="https://unpkg.com/@google/model-viewer/dist/model-viewer.js"></script>
Other Info	
Instances	2
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	<a href="#">829</a>
WASC Id	15
Plugin Id	<a href="#">10017</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>

Low	Strict-Transport-Security Header Not Set
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	<a href="https://thethrone.in">https://thethrone.in</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://thethrone.in/cdn-cgi">https://thethrone.in/cdn-cgi</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://thethrone.in/cdn-cgi/styles">https://thethrone.in/cdn-cgi/styles</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://thethrone.in/cdn-cgi/styles/cf.errors.css">https://thethrone.in/cdn-cgi/styles/cf.errors.css</a>
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	<a href="https://thethrone.in/cdn-cgi/styles/cf.errors.ie.css">https://thethrone.in/cdn-cgi/styles/cf.errors.ie.css</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://thethrone.in/robots.txt">https://thethrone.in/robots.txt</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	<a href="https://thethrone.in/sitemap.xml">https://thethrone.in/sitemap.xml</a>
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	8
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	<a href="https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html</a> <a href="https://owasp.org/www-community/Security-Headers">https://owasp.org/www-community/Security-Headers</a> <a href="https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security">https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security</a> <a href="https://caniuse.com/stricttransportsecurity">https://caniuse.com/stricttransportsecurity</a> <a href="https://datatracker.ietf.org/doc/html/rfc6797">https://datatracker.ietf.org/doc/html/rfc6797</a>
CWE Id	<a href="#">319</a>
WASC Id	15
Plugin Id	<a href="#">10035</a>



Low	Timestamp Disclosure - Unix
Description	A timestamp was disclosed by the application/web server. - Unix
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	1478001846
Other Info	1478001846, which evaluates to: 2016-11-01 17:34:06.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	1729863339
Other Info	1729863339, which evaluates to: 2024-10-25 19:05:39.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	1729869869
Other Info	1729869869, which evaluates to: 2024-10-25 20:54:29.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	1729869923
Other Info	1729869923, which evaluates to: 2024-10-25 20:55:23.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	1729871768
Other Info	1729871768, which evaluates to: 2024-10-25 21:26:08.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>

Method	GET
Parameter	
Attack	
Evidence	1729871915
Other Info	1729871915, which evaluates to: 2024-10-25 21:28:35.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	1729875707
Other Info	1729875707, which evaluates to: 2024-10-25 22:31:47.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	1729875746
Other Info	1729875746, which evaluates to: 2024-10-25 22:32:26.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	1729877982
Other Info	1729877982, which evaluates to: 2024-10-25 23:09:42.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	1729878089
Other Info	1729878089, which evaluates to: 2024-10-25 23:11:29.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	1729943922

Other Info	1729943922, which evaluates to: 2024-10-26 17:28:42.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	1742395481
Other Info	1742395481, which evaluates to: 2025-03-19 20:14:41.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	1744896648
Other Info	1744896648, which evaluates to: 2025-04-17 19:00:48.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	server-timing
Attack	
Evidence	1744897932
Other Info	1744897932, which evaluates to: 2025-04-17 19:22:12.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	x-request-id
Attack	
Evidence	1744897932
Other Info	1744897932, which evaluates to: 2025-04-17 19:22:12.
Instances	15
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	<a href="https://cwe.mitre.org/data/definitions/200.html">https://cwe.mitre.org/data/definitions/200.html</a>
CWE Id	<a href="#">497</a>
WASC Id	13
Plugin Id	<a href="#">10096</a>

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

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//cdn.shopify.com/shopifycloud/storefront-forms-hcaptcha/ce_storefront_forms_captcha_hcaptcha.v1.5.2.iife.js',D={infoText:'Prote", see evidence field for the suspicious comment/snippet.
Instances	1
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	<a href="#">615</a>
WASC Id	13
Plugin Id	<a href="#">10027</a>

Informational	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	<a href="http://testphp.vulnweb.com/AJAX/index.php">http://testphp.vulnweb.com/AJAX/index.php</a>
Method	GET
Parameter	
Attack	
Evidence	<code>&lt;a href="#" onclick="loadSomething('titles.php')"&gt;titles&lt;/a&gt;</code>
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	<code>&lt;a href="#" onClick="window.open('./comment.php?aid=1','comment','width=500,height=400')"&gt;comment on this artist&lt;/a&gt;</code>
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	<code>&lt;a href="#" onClick="window.open('./comment.php?aid=1','comment','width=500,height=400')"&gt;comment on this artist&lt;/a&gt;</code>
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	<code>&lt;a href="#" onClick="window.open('./comment.php?aid=2','comment','width=500,height=400')"&gt;comment on this artist&lt;/a&gt;</code>
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	<code>&lt;a href='#' onClick="window.open('./comment.php?aid=3','comment','width=500,height=400')"&gt;comment on this artist&lt;/a&gt;</code>
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	<code>&lt;a href='#' onClick="window.open('./comment.php?pid=1','comment','width=500,height=400')"&gt;comment on this picture&lt;/a&gt;</code>
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	<code>&lt;a href='#' onClick="window.open('./comment.php?pid=7','comment','width=500,height=400')"&gt;comment on this picture&lt;/a&gt;</code>
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	<code>&lt;a href='#' onClick="window.open('./comment.php?pid=1','comment','width=500,height=400')"&gt;comment on this picture&lt;/a&gt;</code>
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	<code>&lt;a href='#' onClick="window.open('./comment.php?pid=6','comment','width=500,height=400')"&gt;comment on this picture&lt;/a&gt;</code>

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="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	<a class="frontpage-menu-link" href=""></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	10
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	<a href="#">10109</a>



Informational	Re-examine Cache-control Directives
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	cache-control
Attack	
Evidence	
Other Info	
Instances	1
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	<a href="https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching">https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching</a> <a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control</a> <a href="https://grayduck.mn/2021/09/13/cache-control-recommendations/">https://grayduck.mn/2021/09/13/cache-control-recommendations/</a>
CWE Id	<a href="#">525</a>
WASC Id	13
Plugin Id	<a href="#">10015</a>

Informational	Retrieved from Cache
Description	<p>The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.</p>
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	
Attack	
Evidence	hit
Other Info	
Instances	1
Solution	<p>Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:</p> <p>Cache-Control: no-cache, no-store, must-revalidate, private</p> <p>Pragma: no-cache</p> <p>Expires: 0</p> <p>This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.</p>
Reference	<a href="https://tools.ietf.org/html/rfc7234">https://tools.ietf.org/html/rfc7234</a> <a href="https://tools.ietf.org/html/rfc7231">https://tools.ietf.org/html/rfc7231</a> <a href="https://www.rfc-editor.org/rfc/rfc9110.html">https://www.rfc-editor.org/rfc/rfc9110.html</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10050</a>

Informational	Session Management Response Identified
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	<a href="https://thethrone.in/">https://thethrone.in/</a>
Method	GET
Parameter	_shopify_y
Attack	
Evidence	49FC799E-9a05-47AD-9a19-8f3906de213c
Other Info	cookie:_shopify_y cookie:_shopify_s cookie:_tracking_consent
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/session-mgmt-id">https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10112</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

