Sites: http://testphp.vulnweb.com https://thethrone.in

Generated on Fri, 18 Apr 2025 00:09:14

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	8
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
Absence of Anti-CSRF Tokens	Medium	44
CSP: Failure to Define Directive with No Fallback	Medium	1
CSP: Wildcard Directive	Medium	1
CSP: script-src unsafe-inline	Medium	1
CSP: style-src unsafe-inline	Medium	1
Content Security Policy (CSP) Header Not Set	Medium	72
Directory Browsing	Medium	3
Missing Anti-clickjacking Header	Medium	51
Cookie No HttpOnly Flag	Low	4
Cookie Without Secure Flag	Low	6
Cookie without SameSite Attribute	Low	1
Cross-Domain JavaScript Source File Inclusion	Low	2
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	67
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	100
Strict-Transport-Security Header Not Set	Low	8
Timestamp Disclosure - Unix	Low	15
X-Content-Type-Options Header Missing	Low	76
Authentication Request Identified	Informational	1
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	35
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	11
Re-examine Cache-control Directives	Informational	1
Retrieved from Cache	Informational	1
Session Management Response Identified	Informational	1
User Controllable HTML Element Attribute (Potential XSS)	Informational	3

Alert Detail

Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://testphp.vulnweb.com
Method	GET
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	http://testphp.vulnweb.com/
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	http://testphp.vulnweb.com/artists.php	
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	http://testphp.vulnweb.com/artists.php?artist=1	
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	http://testphp.vulnweb.com/artists.php?artist=2	
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	http://testphp.vulnweb.com/artists.php?artist=3	
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		http://testphp.vulnweb.com/cart.php
	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		http://testphp.vulnweb.com/categories.php
	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		http://testphp.vulnweb.com/disclaimer.php
	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		http://testphp.vulnweb.com/guestbook.php
	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	http://testphp.vulnweb.com/guestbook.php
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	http://testphp.vulnweb.com/index.php
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	http://testphp.vulnweb.com/listproducts.php?artist=1
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	http://testphp.vulnweb.com/listproducts.php?artist=2
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	http://testphp.vulnweb.com/listproducts.php?artist=3	
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	http://testphp.vulnweb.com/listproducts.php?cat=1	
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	http://testphp.vulnweb.com/listproducts.php?cat=2	
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	http://testphp.vulnweb.com/listproducts.php?cat=3	
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		http://testphp.vulnweb.com/listproducts.php?cat=4
	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		http://testphp.vulnweb.com/login.php
	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		http://testphp.vulnweb.com/login.php
	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		http://testphp.vulnweb.com/product.php?pic=1
	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	http://testphp.vulnweb.com/product.php?pic=1	
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	http://testphp.vulnweb.com/product.php?pic=2	
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	http://testphp.vulnweb.com/product.php?pic=2	
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	http://testphp.vulnweb.com/product.php?pic=3	
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	http://testphp.vulnweb.com/product.php?pic=3
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	http://testphp.vulnweb.com/product.php?pic=4
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	http://testphp.vulnweb.com/product.php?pic=4
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	http://testphp.vulnweb.com/product.php?pic=5
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	http://testphp.vulnweb.com/product.php?pic=5
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	http://testphp.vulnweb.com/product.php?pic=6
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	http://testphp.vulnweb.com/product.php?pic=6
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	http://testphp.vulnweb.com/product.php?pic=7
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	http://testphp.vulnweb.com/product.php?pic=7
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	http://testphp.vulnweb.com/search.php?test=query
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	http://testphp.vulnweb.com/signup.php
Method	GET
Parameter	
Attack	
Evidence	<form name="form1" method="post" action="/secured/newuser.php">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "signup" "ucc" "uemail" "upass" "upass2" "uphone" "urname" "uuname"].
URL	http://testphp.vulnweb.com/signup.php
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	https://thethrone.in/	
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	https://thethrone.in/	
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	http://testphp.vulnweb.com/cart.php	
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	http://testphp.vulnweb.com/guestbook.php
	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	http://testphp.vulnweb.com/guestbook.php
	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	http://testphp.vulnweb.com/search.php?test=query
	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	44	
Solution		Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

	Phase: Architecture and Design
	Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).
	Note that this can be bypassed using XSS.
	Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.
	Note that this can be bypassed using XSS.
	Use the ESAPI Session Management control.
	This control includes a component for CSRF.
	Do not use the GET method for any request that triggers a state change.
	Phase: Implementation
	Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	CSP: Failure to Define Directive with No Fallback
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	https://thethrone.in/
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	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/ csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

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	https://thethrone.in/
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	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

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	https://thethrone.in/
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	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

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	https://thethrone.in/
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	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

Medium	Content Security Policy (CSP) Header Not Set
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://testphp.vulnweb.com
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php
Method	GET

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

URL	http://testphp.vulnweb.com/disclaimer.php	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Flash/	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/guestbook.php	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/high	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/hpp/	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/hpp/?pp=12	
Method	GET	
Parameter		
Attack		

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

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

URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3	
Method	GET	
Parameter		
Attack		

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink

Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/	
Method	GET	
Parameter		

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

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

Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Parameter	

Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://thethrone.in
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://thethrone.in/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://thethrone.in/cdn-cgi
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://thethrone.in/cdn-cgi/styles
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://thethrone.in/robots.txt

Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	https://thethrone.in/sitemap.xml	
Method	GET	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/cart.php	
Method	POST	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/guestbook.php	
Method	POST	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/search.php?test=query	
Method	POST	
Parameter		
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/secured/newuser.php	
Method	POST	
Parameter		
Attack		
Evidence		

Other Info	
Instances	72
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/ Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/ Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	Directory Browsing
Description	It is possible to view a listing of the directory contents. Directory listings may reveal hidden scripts, include files, backup source files, etc., which can be accessed to reveal sensitive information.
URL	http://testphp.vulnweb.com/Flash/
Method	GET
Parameter	
Attack	
Evidence	<title>Index of /Flash/</title>
Other Info	Web server identified: Apache 2
URL	http://testphp.vulnweb.com/images/
Method	GET
Parameter	
Attack	
Evidence	<title>Index of /images/</title>
Other Info	Web server identified: Apache 2
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/
Method	GET
Parameter	
Attack	
Evidence	<title>Index of /Mod_Rewrite_Shop/images/</title>
Other Info	Web server identified: Apache 2
Instances	3
Solution	Configure the web server to disable directory browsing.
Reference	https://cwe.mitre.org/data/definitions/548.html
CWE Id	548
WASC Id	16
Plugin Id	10033

Medium	Missing Anti-clickjacking Header
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	http://testphp.vulnweb.com
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php
Method	GET
Parameter	x-frame-options
Attack	
Evidence	

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

Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/?pp=12
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/images/

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

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

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

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

Evidence		
Other Info		
URL	http://testphp.vulnweb.com/product.php?pic=3	
Method	GET	
Parameter	x-frame-options	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/product.php?pic=4	
Method	GET	
Parameter	x-frame-options	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/product.php?pic=5	
Method	GET	
Parameter	x-frame-options	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/product.php?pic=6	
Method	GET	
Parameter	x-frame-options	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/product.php?pic=7	
Method	GET	
Parameter	x-frame-options	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/search.php?test=query	
Method	GET	

Parameter	x-frame-options	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/secured/newuser.php	
Method	GET	
Parameter	x-frame-options	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/signup.php	
Method	GET	
Parameter	x-frame-options	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/cart.php	
Method	POST	
Parameter	x-frame-options	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/guestbook.php	
Method	POST	
Parameter	x-frame-options	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/search.php?test=query	
Method	POST	
Parameter	x-frame-options	
Attack		
Evidence		
Other Info		

URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
Instances	51
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Low	Cookie No HttpOnly Flag
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	https://thethrone.in/
Method	GET
Parameter	_shopify_s
Attack	
Evidence	set-cookie: _shopify_s
Other Info	
URL	https://thethrone.in/
Method	GET
Parameter	_shopify_y
Attack	
Evidence	set-cookie: _shopify_y
Other Info	
URL	https://thethrone.in/
Method	GET
Parameter	_tracking_consent
Attack	
Evidence	set-cookie: _tracking_consent
Other Info	
URL	https://thethrone.in/
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	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13

Plugin Id	[10010](10010)

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	https://thethrone.in/
Method	GET
Parameter	_landing_page
Attack	
Evidence	set-cookie: _landing_page
Other Info	
URL	https://thethrone.in/
Method	GET
Parameter	_orig_referrer
Attack	
Evidence	set-cookie: _orig_referrer
Other Info	
URL	https://thethrone.in/
Method	GET
Parameter	_shopify_s
Attack	
Evidence	set-cookie: _shopify_s
Other Info	
URL	https://thethrone.in/
Method	GET
Parameter	_shopify_y
Attack	
Evidence	set-cookie: _shopify_y
Other Info	
URL	https://thethrone.in/
Method	GET
Parameter	_tracking_consent
Attack	
Evidence	set-cookie: _tracking_consent
Other Info	

URL	https://thethrone.in/
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	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
CWE Id	614
WASC Id	13
Plugin Id	10011

Low	Cookie without SameSite Attribute
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://thethrone.in/
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	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	Cross-Domain JavaScript Source File Inclusion
Description	The page includes one or more script files from a third-party domain.
URL	https://thethrone.in/
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	https://thethrone.in/
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	829
WASC Id	15
Plugin Id	10017

Low	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	http://testphp.vulnweb.com
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/artists.php
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

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

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

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

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

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

URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html	
Method	GET	
Parameter		
Attack		
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1	
Other Info		
URL	http://testphp.vulnweb.com/privacy.php	
Method	GET	
Parameter		
Attack		
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1	
Other Info		
URL	http://testphp.vulnweb.com/product.php?pic=1	
Method	GET	
Parameter		
Attack		
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1	
Other Info		
URL	http://testphp.vulnweb.com/product.php?pic=2	
Method	GET	
Parameter		
Attack		
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1	
Other Info		
URL	http://testphp.vulnweb.com/product.php?pic=3	
Method	GET	
Parameter		
Attack		
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1	
Other Info		
URL	http://testphp.vulnweb.com/product.php?pic=4	
Method	GET	
Parameter		
Attack		

Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/secured/
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	GET

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

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

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

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

Other Info	
Instances	67
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id	497
WASC Id	13
Plugin Id	10037

Low	Server Leaks Version Information via "Server" HTTP Response Header Field
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	http://testphp.vulnweb.com
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0

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

Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/categories.php	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/disclaimer.php	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/Flash	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/Flash/	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/Flash/add.fla	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/Flash/add.swf	

Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/guestbook.php	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/high	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/hpp	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/hpp/	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/hpp/?pp=12	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	

Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/images
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/images/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/images/logo.gif
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/images/remark.gif
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/index.php
Method	GET
Parameter	

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

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

Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Method	GET
Parameter	

Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0

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

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

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

Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/secured
Method	GET

Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/secured/
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/secured/style.css
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0

Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
Method	GET
Parameter	
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
Method	GET
Parameter	

Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&size=160	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160	
Method	GET	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg	

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

Other Info		
URL	http://testphp.vulnweb.com/cart.php	
Method	POST	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/guestbook.php	
Method	POST	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/search.php?test=query	
Method	POST	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/secured/newuser.php	
Method	POST	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/userinfo.php	
Method	POST	
Parameter		
Attack		
Evidence	nginx/1.19.0	
Other Info		
Instances	100	
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.	

Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10036

Low	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	https://thethrone.in
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://thethrone.in/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://thethrone.in/cdn-cgi
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://thethrone.in/cdn-cgi/styles
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://thethrone.in/cdn-cgi/styles/cf.errors.css
Method	GET
Parameter	
Attack	

	Evidence	
	Other Info	
URL		https://thethrone.in/cdn-cgi/styles/cf.errors.ie.css
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://thethrone.in/robots.txt
	Method	GET
	Parameter	
	Attack	
	Evidence	
	Other Info	
URL		https://thethrone.in/sitemap.xml
	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		https://cheatsheetseries.owasp.org/cheatsheets/ HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id		319
WASC Id		15
Plugin Id		10035

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

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

Other Info	1729943922, which evaluates to: 2024-10-26 17:28:42.	
URL	https://thethrone.in/	
Method	GET	
Parameter		
Attack		
Evidence	1742395481	
Other Info	1742395481, which evaluates to: 2025-03-19 20:14:41.	
URL	https://thethrone.in/	
Method	GET	
Parameter		
Attack		
Evidence	1744896648	
Other Info	1744896648, which evaluates to: 2025-04-17 19:00:48.	
URL	https://thethrone.in/	
Method	GET	
Parameter	server-timing	
Attack		
Evidence	1744897932	
Other Info	1744897932, which evaluates to: 2025-04-17 19:22:12.	
URL	https://thethrone.in/	
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	https://cwe.mitre.org/data/definitions/200.html	
CWE Id	497	
WASC Id	13	
Plugin Id	10096	

Low	X-Content-Type-Options Header Missing
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://testphp.vulnweb.com
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	http://testphp.vulnweb.com/
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	http://testphp.vulnweb.com/AJAX/
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	http://testphp.vulnweb.com/AJAX/index.php
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	http://testphp.vulnweb.com/AJAX/styles.css	
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	http://testphp.vulnweb.com/artists.php	
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	http://testphp.vulnweb.com/artists.php?artist=1	
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	http://testphp.vulnweb.com/artists.php?artist=2	
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	http://testphp.vulnweb.com/artists.php?artist=3	
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	http://testphp.vulnweb.com/cart.php	
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	http://testphp.vulnweb.com/categories.php	
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	http://testphp.vulnweb.com/disclaimer.php	
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		http://testphp.vulnweb.com/Flash/
	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		http://testphp.vulnweb.com/Flash/add.fla
	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		http://testphp.vulnweb.com/Flash/add.swf
	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		http://testphp.vulnweb.com/guestbook.php
	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	http://testphp.vulnweb.com/hpp/	
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	http://testphp.vulnweb.com/hpp/?pp=12	
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	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12	
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	http://testphp.vulnweb.com/images/	
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	http://testphp.vulnweb.com/images/logo.gif	
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		http://testphp.vulnweb.com/images/remark.gif
	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		http://testphp.vulnweb.com/index.php
	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		http://testphp.vulnweb.com/listproducts.php?artist=1
	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		http://testphp.vulnweb.com/listproducts.php?artist=2
	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	http://testphp.vulnweb.com/listproducts.php?artist=3
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	http://testphp.vulnweb.com/listproducts.php?cat=1
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	http://testphp.vulnweb.com/listproducts.php?cat=2
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	http://testphp.vulnweb.com/listproducts.php?cat=3
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		http://testphp.vulnweb.com/listproducts.php?cat=4
	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		http://testphp.vulnweb.com/login.php
	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		http://testphp.vulnweb.com/Mod_Rewrite_Shop/
	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		http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
	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		http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/
	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		http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/
	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		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/
	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		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/
	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	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/	
	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	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/	
	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	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/1.jpg	
	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	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/2.jpg	
	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	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/3.jpg	
	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	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html	
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	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html	
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	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html	
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	http://testphp.vulnweb.com/product.php?pic=1	
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	http://testphp.vulnweb.com/product.php?pic=2
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	http://testphp.vulnweb.com/product.php?pic=3
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	http://testphp.vulnweb.com/product.php?pic=4
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	http://testphp.vulnweb.com/product.php?pic=5
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		http://testphp.vulnweb.com/product.php?pic=6
	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		http://testphp.vulnweb.com/product.php?pic=7
	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		http://testphp.vulnweb.com/search.php?test=query
	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		http://testphp.vulnweb.com/secured/newuser.php
	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		http://testphp.vulnweb.com/secured/style.css
	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		http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'
	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		http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
	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		http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
	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	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
	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	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
	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	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
	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	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
	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	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
	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	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160	
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	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg	
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	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&size=160	
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	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg	
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	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160	
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	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg	
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	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&size=160	
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	http://testphp.vulnweb.com/signup.php	
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		http://testphp.vulnweb.com/style.css
	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		http://testphp.vulnweb.com/cart.php
	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		http://testphp.vulnweb.com/guestbook.php
	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		http://testphp.vulnweb.com/search.php?test=query
	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	http://testphp.vulnweb.com/secured/newuser.php
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	76
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	Authentication Request Identified
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	http://testphp.vulnweb.com/secured/newuser.php
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	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	Charset Mismatch (Header Versus Meta Content-Type Charset)
Description	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set. An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.
URL	http://testphp.vulnweb.com
Method	GET
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	http://testphp.vulnweb.com/
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	http://testphp.vulnweb.com/AJAX/
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	http://testphp.vulnweb.com/AJAX/index.php
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	http://testphp.vulnweb.com/artists.php	
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	http://testphp.vulnweb.com/artists.php?artist=1	
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	http://testphp.vulnweb.com/artists.php?artist=2	
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	http://testphp.vulnweb.com/artists.php?artist=3	
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	http://testphp.vulnweb.com/cart.php	
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	http://testphp.vulnweb.com/categories.php	
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	http://testphp.vulnweb.com/disclaimer.php	
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	http://testphp.vulnweb.com/guestbook.php	
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	http://testphp.vulnweb.com/index.php	
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	http://testphp.vulnweb.com/listproducts.php?artist=1	
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	http://testphp.vulnweb.com/listproducts.php?artist=2
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	http://testphp.vulnweb.com/listproducts.php?artist=3
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	http://testphp.vulnweb.com/listproducts.php?cat=1
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	http://testphp.vulnweb.com/listproducts.php?cat=2
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	http://testphp.vulnweb.com/listproducts.php?cat=3
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	http://testphp.vulnweb.com/listproducts.php?cat=4	
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	http://testphp.vulnweb.com/login.php	
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	http://testphp.vulnweb.com/product.php?pic=1	
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	http://testphp.vulnweb.com/product.php?pic=2	
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	http://testphp.vulnweb.com/product.php?pic=3	
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	http://testphp.vulnweb.com/product.php?pic=4
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	http://testphp.vulnweb.com/product.php?pic=5
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	http://testphp.vulnweb.com/product.php?pic=6
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	http://testphp.vulnweb.com/product.php?pic=7
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	http://testphp.vulnweb.com/search.php?test=query
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	http://testphp.vulnweb.com/secured/newuser.php	
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	http://testphp.vulnweb.com/signup.php	
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	http://testphp.vulnweb.com/cart.php	
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	http://testphp.vulnweb.com/guestbook.php	
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	http://testphp.vulnweb.com/search.php?test=query	
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	http://testphp.vulnweb.com/secured/newuser.php
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	35
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id	436
WASC Id	15
Plugin Id	90011

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.
URL	https://thethrone.in/
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	615
WASC Id	13
Plugin Id	10027

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

Parameter	
Attack	
Evidence	comment on this artist
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/artists.php?artist=3
Method	GET
Parameter	
Attack	
Evidence	comment on this artist
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET
Parameter	
Attack	
Evidence	comment on this picture
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Parameter	
Attack	
Evidence	comment on this picture
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET
Parameter	
Attack	
Evidence	comment on this picture
Other Info	

		Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL		http://testphp.vulnweb.com/listproducts.php?cat=2
	Method	GET
	Parameter	
	Attack	
	Evidence	comment on this picture
	Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL		https://thethrone.in/
	Method	GET
	Parameter	
	Attack	
	Evidence	
	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		11
Solution		This is an informational alert and so no changes are required.
Reference		
CWE Id		
WASC Id		
Plugin Id		10109

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	https://thethrone.in/
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	https://cheatsheetseries.owasp.org/cheatsheets/ Session_Management_Cheat_Sheet.html#web-content-caching https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	Retrieved from Cache
Description	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.
URL	https://thethrone.in/
Method	GET
Parameter	
Attack	
Evidence	hit
Other Info	
Instances	1
Solution	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: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 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.
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 https://www.rfc-editor.org/rfc/rfc9110.html
CWE Id	
WASC Id	
Plugin Id	10050

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	https://thethrone.in/
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	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id
CWE Id	
WASC Id	
Plugin Id	10112

Informational	User Controllable HTML Element Attribute (Potential XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
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: http://testphp.vulnweb.com/guestbook.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: submit=add message The user-controlled value was: add message
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	goButton
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://testphp.vulnweb.com/search.php?test=query appears to include user input in: a(n) [input] tag [name] attribute The user input found was: goButton=go The user-controlled value was: gobutton
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Parameter	goButton
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://testphp.vulnweb.com/search.php?test=query appears to include user input in: a(n) [input] tag [value] attribute The user input found was: goButton=go The user-controlled value was: go
Instances	3
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	

	https://cheatsheetseries.owasp.org/cheatsheets/ Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031

Sequence Details

With the associated active scan results.

Report generated by VirtuesTech Security Scanner