

Target: http://testphp.vulnweb.com

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

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

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

ZAP Version: 2.16.1

Summary of Alerts

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

Alerts

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

Passing Rules

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ZAP is Out of Date	Passive	MEDIUM	-

Vulnerable US Library (Powered by Redro js) Cooke No HimChity Flag Passive MEDIUM Cooke No HimChity Flag Passive MEDIUM Cooke No HimChity Flag Research Flag	Insecure JSF ViewState	Passive	MEDIUM	_
Re-examine Carche-control Directives Re-examine Carche-control Directives Re-examine Carche-control Directives Resolve MEDIUM RESOlve RESOlve RESOlve Resolve Information in URL Resolve MEDIUM RESOlve			MEDIUM	-
Re-examine Cache-control Directives Cross-Domain JavaScriot Source File Inclusion Cross-Domain JavaScriot Source File Inclusion Passive MEDIUM Cross-Domain JavaScriot Source File Inclusion Passive MEDIUM Information Disclosure - Debug Error Messages Information Disclosure - Sensitive Information in URL Information Disclosure - Sensitive Information in HTTP Referrer Header Information Disclosure - Sensitive Information in HTTP Referrer Header Information Disclosure - Sensitive Information in HTTP Referrer Header Information Disclosure - Sensitive Information in HTTP Referrer Header Information Disclosure - Sensitive Information in HTTP Referrer Header Information Disclosure - Sensitive Information in HTTP Referrer Header Information Disclosure - Sensitive Information in HTTP Referrer Header Information Disclosure - Sensitive Information in HTTP Referrer Header Passive MEDIUM - Disclosure Disclosure - Sensitive Information Leak Passive MEDIUM - Disclosure Pages MEDIUM - Disclosure Pages Include Meed Content Passive MEDIUM - Secure Pages Include Meed Content Passive MEDIUM - HTTP In HTTPS Insecure Transition in Form Post HTTP In HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTP In HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTP In HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTP In HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTP In HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTP In HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTP In HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTP In HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTP In HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTP In HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTP In HTTPS Insecure Transition in Form Post Passive MEDI		Passive	MEDIUM	-
Cross-Domain JavaScript Source File Inclusion Passive MEDIUM - Content-Type Header Missing Passive MEDIUM - Application Error Disclosure Petud Error Messages Passive MEDIUM - Information Disclosure - Debug Error Messages Passive MEDIUM - Information Disclosure - Sensitive Information in URL Passive MEDIUM - Information Disclosure - Sensitive Information in URL Passive MEDIUM - Information Disclosure - Sensitive Information in HTTP Reterrer Header Information Disclosure - Sensitive Information in HTTP Reterrer Header Passive MEDIUM - Information Disclosure - Suspicious Comments Passive MEDIUM - Cookie Prisonning Passive MEDIUM - Cookie Prisonning Passive MEDIUM - Selectorical Passive MEDIUM - Selectorical Passive MEDIUM - WSDL File Detection Passive MEDIUM - Uses Controllable Charset Passive MEDIUM - Passive MEDIUM - Selectorical Passive MEDIUM - Directory Browsing Passive MEDIUM - Passive MEDIUM - Passive MEDIUM - Directory Browsing Passive MEDIUM - Passive MED	Cookie Without Secure Flag	Passive	MEDIUM	-
Content Type Header Missing	Re-examine Cache-control Directives	Passive	MEDIUM	-
Application Error Disclosure Passive MEDIUM . Information Disclosure - Dobug Error Messages Passive MEDIUM . Information Disclosure - Sensitive Information in URL . Information Disclosure - Sensitive Information in URL . Information Disclosure - Sensitive Information in HTTP Referrer Header . Information Disclosure - Suspicious Comments . Off-site Redirect . Passive MEDIUM . Disclosure - Suspicious Comments . Passive MEDIUM . Disclosure - Suspicious Comments . Passive MEDIUM . Disclosure - Suspicious Comments . Passive MEDIUM . Disclosure - Suspicious . Passive MEDIUM . Disclosure - Suspicious . Disclosure - Passive . Disclosure - Suspicious . Description - Suspicious . Disclosure - Suspicious . Disclosure - Passive . Disclosure - Suspicious	Cross-Domain JavaScript Source File Inclusion	Passive	MEDIUM	-
Information Disclosure - Debug Error Messages Information Disclosure - Sensitive Information IURL Passive MEDIUM Information Disclosure - Sensitive Information in URL Information Disclosure - Sensitive Information Disclosure - Sensitive Information Disclosure - MEDIUM - Dessive M	Content-Type Header Missing	Passive	MEDIUM	-
Information Disclosure - Sensitive Information IURL Information Disclosure - Sensitive Information IHTP Referrer Header Information Disclosure - Sensitive Information IHTP Referrer Header Information Disclosure - Suspicious Comments Off site Reducet Passive MEDIUM - Cookie Poisoning Passive MEDIUM - User Controllable Charser Passive MEDIUM - User Controllable Charser Passive MEDIUM - Loosely Scoped Cookie Passive MEDIUM - Strict-Transport-Security Header Passive MEDIUM - Loosely Scoped Cookie Passive MEDIUM - Lookie without SameSile Attribute - Pas	Application Error Disclosure	Passive	MEDIUM	-
Information Disclosure - Sensitive Information in HTTP Referrer Header Information Disclosure - Suspicious Comments Passive MEDIUM - Cookie Polisoning Passive MEDIUM - Cookie Polisoning Passive MEDIUM - Cookie Polisoning Passive MEDIUM - Disclosure - Suspicious Comments Passive MEDIUM - Cookie Polisoning Passive MEDIUM - Disclosure - Controllable Charset Passive MEDIUM - Cookie Polisoning Passive MEDIUM - Cookie Polisoning Passive MEDIUM - Cookie Polisoning Passive MEDIUM - Cookie Without Sandard Passive MEDIUM - Cookie Without Sandard Passive MEDIUM - Passive MEDIUM - Cookie Without Sandard Passive MEDIUM - Passive MEDIUM - Cookie Without Sandard Passive MEDIUM - Passive MEDIUM - Cookie Without Sandard Passive MEDIUM - Passive MEDIUM - Cookie Without Sandard Passive MEDIUM - Passive MEDIUM - Cookie Without Sandard Passive MEDIUM - Passive MEDIUM - Cookie Without Sandard Passive MEDIUM - Passive MEDIUM - Cookie Without Sandard Passive MEDIUM - Passive MEDIUM - Cookie Without Sandard Passive MEDIUM - Passive MEDIUM - Cookie Without Sandard Passive MEDIUM - Passive MEDIUM - Cookie Without Sandard Passive MEDIUM - Passive MEDIUM - Cookie Without Sandard Passive MEDIUM - Passive MEDIUM - Cookie Without Sandard Passive MEDIUM - Coo	Information Disclosure - Debug Error Messages	Passive	MEDIUM	-
Information Disclosure - Suspicious Comments Off-site Redirect Caokie Poisoning Passive MEDIUM - Caokie Poisoning Passive MEDIUM - User Controllable Charset WSDL File Petection Passive MEDIUM - User Controllable Charset WSDL File Petection Passive MEDIUM - User Controllable Charset WSDL File Petection Passive MEDIUM - User Controllable Charset Passive MEDIUM - Strict-Transport-Security Header Passive MEDIUM - User Controllable JavaScript Event (XSS) Passive MEDIUM - User Controllable JavaScript Event (XSS) Passive MEDIUM - Strict-Transport-Security Header Strict-Transport-Security Header Passive MEDIUM - Controllable JavaScript Event (XSS) Passive MEDIUM - Strict-Transport-Security Information Leak Passive MEDIUM - Strict-Transport-Security Information Information Information In	Information Disclosure - Sensitive Information in URL	Passive	MEDIUM	-
Off-site Redirect Passive MEDIUM - Cooker Poisoning Passive MEDIUM - User Controllable Charset Passive MEDIUM - USOL File Detection Passive MEDIUM - Loosely Scoped Cookie Passive MEDIUM - Viewstate Passive MEDIUM - Directory Browsing Passive MEDIUM - Heartbleed OpenSSL Vulnerability (Indicative) Passive MEDIUM - Strict-Transport-Security Header Passive MEDIUM - X-Backend-Server Header Information Leak Passive MEDIUM - LITTP	Information Disclosure - Sensitive Information in HTTP Referrer Header	Passive	MEDIUM	-
Cookie Poisoning User Controllable Charset Passive MEDIUM - WSDL File Detection Passive MEDIUM - WSDL File Detection Passive MEDIUM - Usosely Scorped Cookie Passive MEDIUM - Directory Browsing Passive MEDIUM - Directory Browsing Passive MEDIUM - Directory Browsing Passive MEDIUM - Strict-Transport-Security Header Passive MEDIUM - Secure Pages Include Mixed Content Passive MEDIUM - HTTP to HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTPS to HTTP Insecure Transition in Form Post Passive MEDIUM - HTTP to Retire Passive MEDIUM - HTTP to Retire Detected (Potential Sensitive Information Leak) Passive MEDIUM - Bio Redirect Detected (Potential Sensitive Information Leak) Passive MEDIUM - Retrieved from Cache Retrieved from Cache Rectire Passive MEDIUM - Retrieved from Cache Rectire Passive MEDIUM - Retrieved from Cache Rectire MEDIUM - Rectire Passive MEDIUM - Rectire MEDIUM - Libedosure Passive MEDIUM - Libedosure MEDIUM - Libedosure MEDIUM - Libedosure MEDIUM - Libedosure MEDIUM - Lib	Information Disclosure - Suspicious Comments	Passive	MEDIUM	-
User Controllable Charset WSDL File Detection Passive MEDIUM Directory Browsing Passive MEDIUM Hearthleed OpenSSL Vulnerability (Indicative) Passive MEDIUM Directory Browsing Passive MEDIUM Strict-Transport-Security Header REGIUM Strict-Transport-Security Header REGIUM Directory Browsing Passive MEDIUM Strict-Transport-Security Header REGIUM Directory Browsing Passive MEDIUM Directory Browsing MEDIUM Directory Browsi	Off-site Redirect	Passive	MEDIUM	-
WSDL File Detection Passive MEDIUM - Loosely Scoped Cookie Passive MEDIUM - Viewstate Passive MEDIUM - Directory Browsing Passive MEDIUM - Hearthleed OpenSSL Vulnerability (Indicative) Passive MEDIUM - Strict-Transport-Security Header Passive MEDIUM - Strict-Transport-Security Header Passive MEDIUM - Strict-Transport-Security Header Passive MEDIUM - Secure Pages Include Mixed Content Passive MEDIUM - HTTP to HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTP to HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTPS In HTP Insecure Transition in Form Post Passive MEDIUM - HTTPS In HTP Insecure Transition in Form Post Passive MEDIUM - User Controllable JavaScript Event (XSS) Passive MEDIUM - User Controllable JavaScript Event (XSS) Passive MEDIUM - Sig Redirect Detected (Potential Sensitive Information Leak) Passive MEDIUM - Cokle without SameSite Attribute Passive MEDIUM - CSP Passive MEDIUM - CSP Passive MEDIUM - CSP Passive MEDIUM - Locokie without SameSite Attribute Passive MEDIUM - CSP Passive MEDIUM - COOKIE WITH COOKIE TO THE CO	Cookie Poisoning	Passive	MEDIUM	-
Loosely Scoped Cookie Viewstate Passive Passive MEDIUM Directory Browsing Passive MEDIUM Passive MEDIUM Passive MEDIUM Passive MEDIUM Passive MEDIUM Strict-Transport-Security Header X-Backend-Server Header Information Leak Passive MEDIUM Pas	<u>User Controllable Charset</u>	Passive	MEDIUM	-
Viewstate Passive MEDIUM - Directory Browsing Passive MEDIUM - Heartbleed OpenSSL Vulnerability (Indicative) Passive MEDIUM - Strict-Transport-Security Header Passive MEDIUM - X-Backend-Server Header Information Leak Passive MEDIUM - Secure Pages include Mixed Content Passive MEDIUM - HTTP to HTTP Insecure Transition in Form Post Passive MEDIUM - HTTPS to HTTP Insecure Transition in Form Post Passive MEDIUM - User Controllable JavaScript Event (XSS) Passive MEDIUM - Big Redirect Detected (Potential Sensitive Information Leak) Passive MEDIUM - Retrieved from Cache Passive MEDIUM - X-Chrome Logger-Data (XCOLD) Header Information Leak Passive MEDIUM - Cookie without SameSite Attribute Passive MEDIUM - CSP Passive MEDIUM - X-Debug-Token Information Leak Passive MEDIUM - Veename Hash Found Passive	WSDL File Detection	Passive	MEDIUM	-
Directory Browsing Passive MEDIUM - Heartbleed OpenSSL Vulnerability (Indicative) Passive MEDIUM - Strict-Transport-Security Header Passive MEDIUM - Strict-Transport-Security Header Passive MEDIUM - Strict-Transport-Security Header Passive MEDIUM - Secure Pages Include Mixed Content Passive MEDIUM - HTTP to HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTP to HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTPS Intervent Transition in Form Post Passive MEDIUM - User Controllable JavaScript Event (XSS) Passive MEDIUM - User Controllable JavaScript Event (XSS) Passive MEDIUM - Big Redirect Detected (Potential Sensitive Information Leak) Passive MEDIUM - Retrieved from Cache Passive MEDIUM - Script Passive MEDIUM - Cookie without SameSite Attribute Passive MEDIUM - Cookie without SameSite Attribute Passive MEDIUM - Script Passive MEDIUM - Username Hash Found Passive MEDIUM - Username Hash Found Passive MEDIUM - Username Hash Found Passive MEDIUM - Pli Disclosure Passive MEDIUM - Pli Disclosure Passive MEDIUM - Script Passive Scan Rule MEDIUM - Stats Passive Scan Rule Passive MEDIUM - Hash Disclosure Passive MEDIUM - Cross-Domain Misconfiguration Passive MEDIUM - Passive MEDIUM - Passive MEDIUM - Cross-Domain Misconfiguration Passive MEDIUM -	Loosely Scoped Cookie	Passive	MEDIUM	-
Heartbleed OpenSSL Vulnerability (Indicative) Passive MEDIUM Strict-Transport-Security Header X-Backend-Server Header Information Leak Passive MEDIUM Passive MEDIUM Passive MEDIUM Passive MEDIUM HTTP to HTTPS Insecure Transition in Form Post HTTPs to HTTP Insecure Transition in Form Post Passive MEDIUM Cookie without SameSite Attribute Passive MEDIUM Passive MEDIUM Passive MEDIUM Passive MEDIUM Passive MEDIUM ACHOMALOGUE PASSIVE MEDIUM Pass	<u>Viewstate</u>	Passive	MEDIUM	-
Strict-Transport-Security Header X.Backend-Server Header Information Leak Passive MEDIUM Passive Passive MEDIUM Passive Passive Passive Passive Passive Pass	<u>Directory Browsing</u>	Passive	MEDIUM	-
X-Backend-Server Header Information Leak Secure Pages Include Mixed Content HTTP to HTTPS Insecure Transition in Form Post Passive MEDIUM HTTP to HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTP to HTTP Insecure Transition in Form Post Passive MEDIUM - User Controllable JavaScript Event (XSS) Passive MEDIUM - Big Redirect Detected (Potential Sensitive Information Leak) Retrieved from Cache Retrieved from Cache Retrieved from Cache Retrieved Information Leak Passive MEDIUM - Cookie without SameSite Attribute Passive MEDIUM - CSP Passive MEDIUM - CSP Passive MEDIUM - Retrieved Information Leak Passive MEDIUM - CSP Passive MEDIUM - RETURN - Subug-Token Information Leak Passive MEDIUM - Response Header Passive MEDIUM - Username Hash Found Response Header Passive MEDIUM - PILI Disclosure Passive MEDIUM - Stats Passive Scan Rules Passive MEDIUM - Stats Passive Scan Rule Passive MEDIUM - Timestamp Disclosure Passive MEDIUM - Timestamp Disclosure Passive MEDIUM - Cross-Domain Misconfiguration Passive MEDIUM - Reverse Tabnabbing MEDIUM - Reverse Tabnabbing	Heartbleed OpenSSL Vulnerability (Indicative)	Passive	MEDIUM	-
Secure Pages Include Mixed Content Passive MEDIUM - HTTP to HTTPS Insecure Transition in Form Post Passive MEDIUM - HTTPS to HTTP Insecure Transition in Form Post Passive MEDIUM - User Controllable JavaScript Event (XSS) Passive MEDIUM - Big Redirect Detected (Potential Sensitive Information Leak) Passive MEDIUM - Retrieved from Cache Passive MEDIUM - X-Chromel agger-Data (XCOLD) Header Information Leak Passive MEDIUM - Cookie without SameSite Attribute Passive MEDIUM - CSP Passive MEDIUM - X-Debug-Token Information Leak Passive MEDIUM - Username Hash Found Passive MEDIUM - X-AspNet-Version Response Header Passive MEDIUM - PIL Disclosure Passive MEDIUM - Script Passive Scan Rules Passive MEDIUM - Stats Passive Scan Rule Passive MEDIUM - Timestamp Disclosure Passive MEDIUM -<	Strict-Transport-Security Header	Passive	MEDIUM	-
HTTP to HTTPS insecure Transition in Form Post Passive MEDIUM - HTTPS to HTTP insecure Transition in Form Post Passive MEDIUM - User Controllable JavaScript Event (XSS) Passive MEDIUM - Big Redirect Detected (Potential Sensitive Information Leak) Passive MEDIUM - Retrieved from Cache Passive MEDIUM - X-ChromeLogger-Data (XCOLD) Header Information Leak Passive MEDIUM - Cookie without SameSite Attribute Passive MEDIUM - CSP Passive MEDIUM - X-Debug-Token Information Leak Passive MEDIUM - Username Hash Found Passive MEDIUM - Username Hash Found Passive MEDIUM - PIL Disclosure Passive MEDIUM - Script Passive Scan Rule Passive MEDIUM - Stats Passive Scan Rule Passive MEDIUM - Timestamp Disclosure Passive MEDIUM - Hash Disclosure Passive MEDIUM - Cross-Domain Misconfiguration Passive MEDIUM - Weak Authentication Method Passive MEDIUM - Reverse Tabnabbing Passive MEDIUM - Reverse Tabnabbing M	X-Backend-Server Header Information Leak	Passive	MEDIUM	-
HTTPS to HTTP Insecure Transition in Form Post User Controllable JavaScript Event (XSS) Passive MEDIUM Retrieved from Cache Retrieved from Cache X-ChromeLogger-Data (XCOLD) Header Information Leak Cookie without SameSite Attribute CSP Passive MEDIUM CSP X-Debug-Token Information Leak Passive MEDIUM Passive MEDIUM CSP X-Debug-Token Information Leak Username Hash Found X-AspNet-Version Response Header PIL Disclosure Passive MEDIUM Passive MEDIUM Passive MEDIUM CSCR X-AspNet-Version Response Header Passive MEDIUM CSCR Passive MEDIUM Passive MEDIUM CSCR Passive MEDIUM CSCR X-AspNet-Version Response Header Passive MEDIUM CSCR Passive MEDIUM CSCR Passive MEDIUM CSCR Passive MEDIUM CSCR Stats Passive Scan Rule Passive MEDIUM CSCR Timestamp Disclosure Passive MEDIUM CTOSS-Domain Misconfiguration Passive MEDIUM CTOSS-Domain Misconfiguration Passive MEDIUM Reverse Tabnabbing	Secure Pages Include Mixed Content	Passive	MEDIUM	-
User Controllable JavaScript Event (XSS) Passive MEDIUM - Big Redirect Detected (Potential Sensitive Information Leak) Passive MEDIUM - Retrieved from Cache Passive MEDIUM - X-ChromeLogger-Data (XCOLD) Header Information Leak Passive MEDIUM - Cookie without SameSite Attribute Passive MEDIUM - CSP Passive MEDIUM - X-Debug-Token Information Leak Passive MEDIUM - Username Hash Found Passive MEDIUM - X-AspNet-Version Response Header Passive MEDIUM - PIL Disclosure Passive MEDIUM - Script Passive Scan Rules Passive MEDIUM - Stats Passive Scan Rule Passive MEDIUM - Timestamp Disclosure Passive MEDIUM - Hash Disclosure Passive MEDIUM - Cross-Domain Misconfiguration Passive MEDIUM - Weak Authentication Method Passive MEDIUM -	HTTP to HTTPS Insecure Transition in Form Post	Passive	MEDIUM	-
Big Redirect Detected (Potential Sensitive Information Leak) Retrieved from Cache X-ChromeLogger-Data (XCOLD) Header Information Leak Passive MEDIUM - Cookie without SameSite Attribute Passive MEDIUM - CSP Passive MEDIUM - X-Debug-Token Information Leak Passive MEDIUM - Username Hash Found Passive MEDIUM - Wesh MEDIUM - Passive MEDIUM - Reverse Tabnabbing - Passive MEDIUM -	HTTPS to HTTP Insecure Transition in Form Post	Passive	MEDIUM	-
Retrieved from Cache X-ChromeLogger-Data (XCOLD) Header Information Leak Passive MEDIUM Cookie without SameSite Attribute Passive MEDIUM CSP Passive MEDIUM - X-Debug-Token Information Leak Passive MEDIUM - Username Hash Found Passive MEDIUM - X-AspNet-Version Response Header Passive MEDIUM - PII Disclosure Passive MEDIUM - Script Passive Scan Rules Passive MEDIUM - Stats Passive Scan Rule Passive MEDIUM - Timestamp Disclosure Passive MEDIUM - Timestamp Disclosure Passive MEDIUM - Reverse Tabnabbing Passive MEDIUM - Reverse Tabnabbing MEDIUM - Resive MEDIUM - Reverse Tabnabbing Passive MEDIUM - MEDI	<u>User Controllable JavaScript Event (XSS)</u>	Passive	MEDIUM	-
X-ChromeLogger-Data (XCOLD) Header Information Leak Passive MEDIUM - Cookie without SameSite Attribute Passive MEDIUM - CSP Passive MEDIUM - X-Debug-Token Information Leak Passive MEDIUM - Username Hash Found Passive MEDIUM - X-AspNet-Version Response Header Passive MEDIUM - PII Disclosure Passive MEDIUM - Script Passive Scan Rules Passive MEDIUM - Stats Passive Scan Rule Passive MEDIUM - Timestamp Disclosure Passive MEDIUM - Hash Disclosure Passive MEDIUM - Cross-Domain Misconfiguration Passive MEDIUM - Weak Authentication Method Passive MEDIUM - Reverse Tabnabbing Passive MEDIUM -	Big Redirect Detected (Potential Sensitive Information Leak)	Passive	MEDIUM	-
Cookie without SameSite Attribute CSP Passive Passive MEDIUM - X-Debug-Token Information Leak Passive MEDIUM - Username Hash Found Passive MEDIUM - X-AspNet-Version Response Header Passive MEDIUM - PII Disclosure Passive MEDIUM - Script Passive Scan Rules Passive MEDIUM - Script Passive Scan Rule Passive MEDIUM - Stats Passive Scan Rule Passive MEDIUM - Cross-Domain Misconfiguration Passive MEDIUM - Cross-Domain Misconfiguration Passive MEDIUM - Weak Authentication Method Passive MEDIUM -	Retrieved from Cache	Passive	MEDIUM	-
CSP X-Debug-Token Information Leak Passive MEDIUM - Username Hash Found Passive MEDIUM - X-AspNet-Version Response Header Passive MEDIUM - PII Disclosure Passive MEDIUM - Script Passive Scan Rules Passive MEDIUM - Stats Passive Scan Rule Passive MEDIUM - Imestamp Disclosure Passive MEDIUM - Timestamp Disclosure Passive MEDIUM - Cross-Domain Misconfiguration Passive MEDIUM - Weak Authentication Method Reverse Tabnabbing Passive MEDIUM - MEDI	X-ChromeLogger-Data (XCOLD) Header Information Leak	Passive	MEDIUM	-
X-Debug-Token Information Leak Username Hash Found Passive MEDIUM - X-AspNet-Version Response Header Passive MEDIUM - PII Disclosure Passive MEDIUM - Script Passive Scan Rules Passive MEDIUM - Stats Passive Scan Rule Passive MEDIUM - Stats Passive MEDIUM - Timestamp Disclosure Passive MEDIUM - Timestamp Disclosure Passive MEDIUM - Cross-Domain Misconfiguration Passive MEDIUM - Weak Authentication Method Passive MEDIUM - Me	Cookie without SameSite Attribute	Passive	MEDIUM	-
Username Hash FoundPassiveMEDIUM-X-AspNet-Version Response HeaderPassiveMEDIUM-PII DisclosurePassiveMEDIUM-Script Passive Scan RulesPassiveMEDIUM-Stats Passive Scan RulePassiveMEDIUM-Timestamp DisclosurePassiveMEDIUM-Hash DisclosurePassiveMEDIUM-Cross-Domain MisconfigurationPassiveMEDIUM-Weak Authentication MethodPassiveMEDIUM-Reverse TabnabbingPassiveMEDIUM-	<u>CSP</u>	Passive	MEDIUM	-
X-AspNet-Version Response HeaderPassiveMEDIUM-PII DisclosurePassiveMEDIUM-Script Passive Scan RulesPassiveMEDIUM-Stats Passive Scan RulePassiveMEDIUM-Timestamp DisclosurePassiveMEDIUM-Hash DisclosurePassiveMEDIUM-Cross-Domain MisconfigurationPassiveMEDIUM-Weak Authentication MethodPassiveMEDIUM-Reverse TabnabbingPassiveMEDIUM-	X-Debug-Token Information Leak	Passive	MEDIUM	-
PII Disclosure Script Passive Scan Rules Passive MEDIUM Stats Passive Scan Rule Passive MEDIUM Timestamp Disclosure Passive MEDIUM Hash Disclosure Passive MEDIUM Cross-Domain Misconfiguration Passive MEDIUM Cross-Domain Misconfiguration Passive MEDIUM Reverse Tabnabbing Passive MEDIUM Passive MEDIUM Passive MEDIUM MEDIUM Passive MEDIUM MEDIUM MEDIUM Passive MEDIUM MEDIUM MEDIUM MEDIUM MEDIUM Passive MEDIUM Reverse Tabnabbing	<u>Username Hash Found</u>	Passive	MEDIUM	-
Script Passive Scan RulesPassiveMEDIUM-Stats Passive Scan RulePassiveMEDIUM-Timestamp DisclosurePassiveMEDIUM-Hash DisclosurePassiveMEDIUM-Cross-Domain MisconfigurationPassiveMEDIUM-Weak Authentication MethodPassiveMEDIUM-Reverse TabnabbingPassiveMEDIUM-	X-AspNet-Version Response Header	Passive	MEDIUM	-
Stats Passive Scan Rule Passive MEDIUM - Timestamp Disclosure Passive MEDIUM - Hash Disclosure Passive MEDIUM - Cross-Domain Misconfiguration Passive MEDIUM - Weak Authentication Method Passive MEDIUM - Reverse Tabnabbing Passive MEDIUM -	<u>PII Disclosure</u>	Passive	MEDIUM	-
Timestamp Disclosure Passive MEDIUM - Hash Disclosure Passive MEDIUM - Cross-Domain Misconfiguration Passive MEDIUM - Weak Authentication Method Passive MEDIUM - Reverse Tabnabbing Passive MEDIUM -	Script Passive Scan Rules	Passive	MEDIUM	-
Hash Disclosure Passive MEDIUM - Cross-Domain Misconfiguration Passive MEDIUM - Weak Authentication Method Passive MEDIUM - Reverse Tabnabbing Passive MEDIUM -	Stats Passive Scan Rule	Passive	MEDIUM	-
Cross-Domain Misconfiguration Passive MEDIUM - Weak Authentication Method Passive MEDIUM - Reverse Tabnabbing Passive MEDIUM -	<u>Timestamp Disclosure</u>	Passive	MEDIUM	-
Weak Authentication Method Passive MEDIUM - Reverse Tabnabbing Passive MEDIUM -		Passive	MEDIUM	-
Reverse Tabnabbing Passive MEDIUM -	Cross-Domain Misconfiguration	Passive	MEDIUM	-
		Passive	MEDIUM	
Modern Web Application Passive MEDIUM -	Reverse Tabnabbing	Passive	MEDIUM	
	Modern Web Application	Passive	MEDIUM	-

Medium	Absence of Anti-CSRF Tokens
	No Anti-CSRF tokens were found in a HTML submission form.
	A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.
Description	CSRF attacks are effective in a number of situations, including:
	* The victim has an active session on the target site.
	* The victim is authenticated via HTTP auth on the target site.
	* The victim is on the same local network as the target site.
	CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://testphp.vulnweb.com/
Method	GET
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
Request Header	GET http://testphp.vulnweb.com/ HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/53 7.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 0K Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:12 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 4958
Response Body (excerpt)	<pre>tent_rgn"> <div id="content"></div></pre>

cliv in - Search -		<div id="navBar"></div>
Comment Comm		<pre><div id="search"> <form action="search php?test=query" method="post"></form></div></pre>
anjust name="golarton" type="subnist" value="go">		<label>search art</label>
Comment Comm		
VINAL http://testph.vulneb.com/arists.php Vinal All http://testph.vulneb.com/arists.php Vinal All http://testph.vulneb.com/arists.php Vinal All http://testph.vulneb.com/arists.php All		
Lis-va href="categories.php">Browse cat Method GET		
URL Method GET Parameter Attack Evidence Slom action="search phip?rest=query" method="post"> No known Ami-CSRF token [anticart, CSRF Token, _csrf_token, _c		
Parameter Attack Evidence cform action="search.php?rest=query" method="post"> No Innover Artic SSRF-plan [anticot, CSSRF-plan [anticot, anticot, anticot, anticot, csrf-plan [anticot, CSSRF-plan [anticot, csrf-plan [anticot	URL	
Attack Evidence	Method	GET
Evidence Cform action="search.php?test=query" method="post"> No known Anti-CSRF loken janics.rf. CSRFTloken,	Parameter	
Other Info Other	Attack	
Other Info carl_tokencarl_carls_carls_carls_carls_carls_carls_tokencarl_tokencarl_tokencarl_tokencarl_tokencarl_tokentokentokentokentokentokentokentokentokentokencarl_tokentokencarl_token	Evidence	<form action="search.php?test=query" method="post"></form>
Method GET Parameter Attack Evidence form action="search.php?test=query" method="post"> No known Anti CSRF token [anticsrf, CSRF-Token, RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_csrf_csrf_csrf_csrf_csrf_csrf_csrf_	Other Info	csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form
Parameter Attack Evidence <pre></pre>	URL	http://testphp.vulnweb.com/artists.php?artist=1
Attack Evidence form action="search.php?test=query" method="post"> No known Anth-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_token, _csrf_token, _csrf_token, _csrf_token, _csrf_token, _data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" searchFor"]. URL Method GET Parameter Attack Evidence form action="search.php?test=query" method="post"> No known Anth-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_token, _csrf_token, _csrf_token, _data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" search.php?test=query" method="post"> URL http://testphp.vu/inweb.com/artists.php?artist=3 Method GET Attack Evidence form action="search.php?test=query" method="post"> No known Anth-CSRF token [anticsrf, CSRFToken, _csrf_token, _csrf_token, _data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" search.php?test=query" method="post"> No known Anth-CSRF token [anticsrf, CSRFToken, _csrf_token, _csrf_token, _data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" search.php?test=query" method="post"> No known Anth-CSRF token [anticsrf, CSRFToken, _csrf_token, _csrf_token, _csrf_token, _athenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_token, _csrf_token, _csrf_token, _csrf_token, _csrf_token, _data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" search.php?test=query" method="post"> No known Anth-CSRF token [anticsrf, CSRFToken, _csrf_token, _csrf_token, _csrf_token, _data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" search.php.vu/inweb.com/cart.php GET	Method	GET
Evidence Storm action="search.php?test=query" method="post"	Parameter	
Other Info No known Anti-CSRF token [anticst, CSRFToken, _Request/verificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_token, _csrf_token, _csrf_token, _csrf_token, _data[_Token [key], _wpnonce] was found in the following HTML form: [Form 1: "go@tuton" search.php?artist=2 Method GET Parameter Attack Evidence ofform action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken, _Request/verificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_token, _csrf_token, _csrf_token, _csrfToken, data[_Token [key], _wpnonce] was found in the following HTML form: [Form 1: "go@tuton" search.php?test=query" method="post"> URL http://lesiphp.vulnweb.com/artists.php?artist=3 Method GET Parameter Attack Evidence ofform action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken, _Request/verificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_token, _csrf_token, _csrf_token, _csrf_token, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_token, _csrf_token, _csrf_token, _csrf_token, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_token, _csrf_token, _csrf_token, _csrf_token, _data[_Token [key], _wpnonce] was found in the following HTML form: [Form 1: "go@utton" "search-For"]; URL http://testphp.vulnweb.com/cart.php Method GET Parameter Altack Altack	Attack	
Other Info csf_lokencsfcsf_scretecsf_magic, CSRFtoken, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] 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"> No known Anti-CSRF token [anticsrf, CSRFToken, _RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrfcsf_token, _csrftoken, _csrftoken, _csrftoken, _csrftoken, _csrf_token, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. URL http://testphp.vulnweb.com/artists.php?artist=3 GET Parameter Attack Evidence form action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken, _RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrftoken, _csrftoken, _csrf	Evidence	<form action="search.php?test=query" method="post"></form>
Method GET Parameter Attack Evidence	Other Info	csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form
Parameter Attack Evidence	URL	http://testphp.vulnweb.com/artists.php?artist=2
Attack Evidence <form action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token,csrf_token,csrf_token,csrfToken, datal_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchEpri"]. URL</form>	Method	GET
Evidence <form action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token,csrf_token,csrf_token,csrf_token,csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor"].</form>	Parameter	
Other Info	Attack	
Other Info csrf_token, _csrf_csrfSecret, _csrf_magic, CSRF, _token, _csrf_token, _data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. Http://testphp.vulnweb.com/artists.php?artist=3 Method GET Parameter Attack Evidence <form action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken, _RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_token, _csrf_token, _csrf_token, _data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. URL http://testphp.vulnweb.com/cart.php Method GET Attack</form>	Evidence	<form action="search.php?test=query" method="post"></form>
Method GET Parameter Attack Evidence <form action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_token, _csrf_token, _csrf_token, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. URL</form>	Other Info	csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form
Parameter Attack Evidence	URL	http://testphp.vulnweb.com/artists.php?artist=3
Attack Evidence <form action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_token, _csrf_token, _csrf_token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. URL</form>	Method	GET
Evidence <form action="search.php?test=query" method="post"> No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_token, _csrf_token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. URL</form>	Parameter	
No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf_token, _csrf_token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. URL http://testphp.vulnweb.com/cart.php GET Attack	Attack	
Other Info csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _data[_Token][key], _wpnonce] 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"></form>
Method GET Parameter Attack	Other Info	csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] was found in the following HTML form: [Form
Parameter Attack	URL	http://testphp.vulnweb.com/cart.php
Attack	Method	GET
	Parameter	
Evidence <form action="search.php?test=query" method="post"></form>	Attack	
	Evidence	<form action="search.php?test=query" method="post"></form>

Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _data[_Token][key], _wpnonce] 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"></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, data[_Token][key], _wpnonce] 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"></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, data[_Token][key], _wpnonce] 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"></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, _data[_Token][key], _wpnonce] 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"></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, _data[_Token][key], _wpnonce] 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"></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, data[_Token][key], _wpnonce] 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"></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, _data[_Token][key], _wpnonce] 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"></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, _data[_Token][key], _wpnonce] 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"></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, data[_Token][key], _wpnonce] 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"></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, data[_Token][key], _wpnonce] 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"></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, data[_Token][key], _wpnonce] 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"></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, data[_Token][key], _wpnonce] 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"></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, _data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/login.php
Method	GET
Parameter	
Attack	
Evidence	<form action="userinfo.php" method="post" name="loginform"></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, data[_Token][key], _wpnonce] 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"></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, _data[_Token][key], _wpnonce] 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 action="cart.php" method="POST" name="f_addcart"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] 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"></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, _data[_Token][key], _wpnonce] 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 action="cart.php" method="POST" name="f_addcart"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] 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"></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, data[_Token][key], _wpnonce] 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 action="cart.php" method="POST" name="f_addcart"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] 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"></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, data[_Token][key], _wpnonce] 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 action="cart.php" method="POST" name="f_addcart"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] 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"></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, data[_Token][key], _wpnonce] 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 action="cart.php" method="POST" name="f_addcart"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] 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"></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, _data[_Token][key], _wpnonce] 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 action="cart.php" method="POST" name="f_addcart"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _csrfToken, data[_Token][key], _wpnonce] 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"></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, _data[_Token][key], _wpnonce] 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 action="cart.php" method="POST" name="f_addcart"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _data[_Token][key], _wpnonce] 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"></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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Parameter	
Attack	
Evidence	<form action="/secured/newuser.php" method="post" name="form1"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _data[_Token][key], _wpnonce] 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"></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, _data[_Token][key], _wpnonce] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Parameter	
Attack	
Evidence	<form action="search.php?test=query" method="post"></form>
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token, _data[_Token][key], _wpnonce] 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"></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, _data[_Token][key], _wpnonce] 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"></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, data[_Token][key], _wpnonce] 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"></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, data[_Token][key], _wpnonce] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
Instances	40
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	<u>352</u>
WASC Id	9
Plugin Id	<u>10202</u>
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	
Request Header	GET http://testphp.vulnweb.com/ HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/5 37.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 0K Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:12 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 4958
Response Body (truncated)	<pre><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false"--> <head> <meta content="text/html; charset=utf-8" http-equiv="Content-Type"/> <!-- InstanceBeginEditable name="document_title_rgn"--> <title>Home of Acunetix Art</title> <!-- InstanceEndEditable--> <!-- InstanceEndEditable--> <!-- InstanceBeginEditable(truncated)</pre--></head></html></pre>
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/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
	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
URL Method	http://testphp.vulnweb.com/listproducts.php?artist=3 GET

Parameter	
Attack	
Evidence	
Other Info	
	http://testphp.vulnweb.com/listproducts.php?cat=1
	GET
Parameter	
Attack	
Evidence	
Other Info	
	http://testphp.vulnweb.com/listproducts.php?cat=2
	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	
	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-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/Details/color-printer/3/
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/2/
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	GET
Attack	
Evidence Other Info	
Other Info	
URL Mathad	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/signup.php
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/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	48
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	<u>693</u>
WASC Id	15
Plugin Id	<u>10038</u>
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
4	

Attack	
Evidence	
Other Info	
Request Header	GET http://testphp.vulnweb.com/ HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/5 37.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 0K Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:12 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 4958
Response Body (truncated)	<pre><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false"--> <head> <meta content="text/html; charset=utf-8" http-equiv="Content-Type"/> <!-- InstanceBeginEditable name="document_title_rgn"--> <title>Home of Acunetix Art</title> <!-- InstanceEndEditable--> <i instanceendeditable=""> <i instancebegineditable(truncated)<="" pre=""></i></i></head></html></pre>
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/guestbook.php
Method	GET
Parameter	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp/
Method	GET
Parameter	x-frame-options

Evidence Other Info	
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/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 X-mame-options	
Evidence	
Other Info	
URL http://testphp.vulnweb.com/listproducts.php?artist=3	
Method GET	
Parameter x-frame-options	
Attack X-mame-options	
Evidence	
Other Info http://teetaha.vulayeb.com/lietareducts.php?cot=1	
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
	GET
	x-frame-options
Attack	
Evidence	
Other Info	
	http://testphp.vulnweb.com/Mod_Rewrite_Shop/
	GET
	x-frame-options
Attack	
Evidence	
Other Info	
	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/
	GET
	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
	x-frame-options
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/
Method	GET
	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
	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/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
	POST
	x-frame-options
Attack	
Evidence	
Other Info	
	http://testphp.vulnweb.com/search.php?test=query
	POST
	x-frame-options
Attack	
Evidence	
Other Info	
	http://testphp.vulnweb.com/secured/newuser.php
	POST
	x-frame-options
Attack	
Evidence	

44
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.
https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options
1021
15
<u>10020</u>
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
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.
http://testphp.vulnweb.com/
GET
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
GET http://testphp.vulnweb.com/ HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/5 37.36 pragma: no-cache cache-control: no-cache
HTTP/1.1 200 0K Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:12 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 4958
<pre><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false"--> <head> <meta content="text/html; charset=utf-8" http-equiv="Content-Type"/> <!-- InstanceBeginEditable name="document_title_rgn"--> <title>Home of Acunetix Art</title> <!-- InstanceEndEditable--> k rel="stylesheet" href="style.css" type="text/css"> <!-- InstanceBeginEditable(truncated)</pre--></head></html></pre>
http://testphp.vulnweb.com/AJAX/index.php

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	

Nethold GET	URL	http://testphp.vulnweb.com/disclaimer.php
Attack Pederone X-Powred By PIP/5.6.40 38-ubuntu/20.0.41-deb.sury.org+1 Other Info URL http://testphp.vulnveb.com/guestbook.php Method GFT Parameter Attack Pederone X-Powred By PIP/5.6.40 38-ubuntu/20.0.41-deb.sury.org+1 Other Info URL http://testphp.vulnveb.com/tipp/pip/fip-12 Attack Pederone X-Powred By PIP/5.6.40 38-ubuntu/20.0.41-deb.sury.org+1 Other Info URL http://testphp.vulnveb.com/tipp//pip-12 Attack Pederone X-Powred By PIP/5.6.40 38-ubuntu/20.0.41-deb.sury.org+1 Other Info URL http://testphp.vulnveb.com/tipp//pip-12 Method GFT Parameter Attack Pederone X-Powred By PIP/5.6.40 38-ubuntu/20.0.41-deb.sury.org+1 Other Info URL http://testphp.vulnveb.com/tipp//pip-12 Attack Pederone X-Powred By PIP/5.6.40 38-ubuntu/20.0.41-deb.sury.org+1 Other Info URL http://testphp.vulnveb.com/tipp/params.php?ps-validapp=12 Attack Pederone X-Powred By PIP/5.6.40 38-ubuntu/20.0.41-deb.sury.org+1 Other Info URL http://testphp.vulnveb.com/tipp/params.php?ps-validapp=12 Attack Pederone X-Powred By PIP/5.6.40 38-ubuntu/20.0.41-deb.sury.org+1 Other Info URL http://testphp.vulnveb.com/index.php Attack Pederone X-Powred By PIP/5.6.40 38-ubuntu/20.0.41-deb.sury.org+1 Other Info URL http://testphp.vulnveb.com/index.php Attack Pederone X-Powred By PIP/5.6.40 38-ubuntu/20.0.41-deb.sury.org+1 Other Info URL http://testphp.vulnveb.com/index.php/params.php?ps-validapp=12 Other Info URL http://testphp.vulnveb.com/index.php/params.php?ps-validapp=1 Other Info URL http://testphp.vulnveb.com/index.php/params.php/params.php?ps-validapp=1 Other Info URL http://testphp.vulnveb.com/index.php/params.	Method	GET
Evidence X-Powered-By: PI-PS 6.40-381-ubuntu20.04.1-deb.sury.org+1 URL Method GET Parameter Attack Evidence X-Powered-By: PI-PS 6.40-38-ubuntu20.04.1-deb.sury.org+1 Other Info URL Muschtestiphs.volimerb.som/bsed Method GET Parameter Attack Evidence X-Powered-By: PI-PS 6.40-38-ubuntu20.04.1-deb.sury.org+1 Other Info URL Muschtestiphs.volimerb.som/bsed Method GET Parameter Attack Evidence X-Powered-By: PI-PS 6.40-38-ubuntu20.04.1-deb.sury.org+1 Other Info URL Muschtestiphs.volimerb.som/bsep3/2ps=12 Method GET Parameter Attack Evidence X-Powered-By: PI-PS 6.40-38-ubuntu20.04.1-deb.sury.org+1 Other Info URL Muschtestiphs.volimerb.som/bsep3/2ps=12 Method GET Parameter Attack Evidence X-Powered-By: PI-PS 6.40-38-ubuntu20.04.1-deb.sury.org+1 Other Info URL Muschtestiphs.volimerb.som/bsep4yar.ams.pths?v=suid-Bous=12 Method GET Parameter Attack Evidence X-Powered-By: PI-PIS 6.40-38-ubuntu20.04.1-deb.sury.org+1 Other Info URL Muschtestiphs.volimerb.som/bsep4yar.ams.pths?v=suid-Bous=12 Method GET Parameter Attack Evidence X-Powered-By: PI-PIS 6.40-38-ubuntu20.04.1-deb.sury.org+1 Other Info URL Muschtestiphs.volimerb.som/bsep4yar.ams.pths?v=suid-Bous=12 Other I	Parameter	
Other Info URL Method GET Parameter Attack Evidence X-Powered-by: PHIPS 0.40-38-shburmu20.041+deb.sury.org+1 Other Info URL Method GET Parameter Attack Evidence X-Powered-by: PHIPS 0.40-38-shburmu20.041+deb.sury.org+1 Other Info URL Mittor. Accidence X-Powered-by: PHIPS 0.40-38-shburmu20.041-deb.sury.org+1 Other Info URL Mittor. Accidence X-Powered-by: PHIPS 0.40-38-shburmu20.041-deb.sury.org+1 Other Info URL Mittor. A	Attack	
URL	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Method GET Parameter Attack Evidence X-Powered-By; PHP/s.6.40-38+ubumn/20.04.1+deb.sury.org+1 Other Info URL Method GET Parameter Attack Evidence X-Powered-By; PHP/s.6.40-38+ubumn/20.04.1+deb.sury.org+1 Other Info URL Method GET Parameter Artack Artack X-Powered-By; PHP/s.6.40-38+ubumn/20.04.1+deb.sury.org+1 Other Info URL Method GET Parameter X-Powered-By; PHP/s.6.40-38+ubumn/20.04.1+deb.sury.org+1 Other Info URL Method GET Parameter Artack Evidence X-Powered-By; PHP/s.6.40-38+ubumn/20.04.1+deb.sury.org+1 Other Info URL Method GET Parameter Artack Evidence X-Powered-By; PHP/s.6.40-38+ubumn/20.04.1+deb.sury.org+1 Other Info Display the permitter of the permitter	Other Info	
Parameter Artack Exidance X-Powered By: PHP/s.6.40.38+ubuniu20.04.1+deb.sury.org+1 Other Info UPL http://mestpho.sc/invesh.com/ligge/ Method GET Parameter Artack Evidance X-Powered By: PHP/s.6.40.38+ubuniu20.04.1+deb.sury.org+1 Other Info UPL UPL http://mestpho.sc/invesh.com/ligge/?ge=12 Method GET Parameter Artack Autuck X Evidance X-Powered By: PHP/s.6.40.38+ubuniu20.04.1-deb.sury.org+1 Other Info Other Info UPL http://ususipho.sc/inveb.com/ligip/params.php?p=valid&pp=12 Method GET Parameter Altuck Evidence X-Powered-By: PHP/s.6.40-38+ubuniu20.04.1-deb.sury.org+1 Other Info GET Parameter Altuck Evidence X-Powered-By: PHP/s.6.40-38+ubuniu20.04.1-deb.sury.org+1 Other Info GET Parameter Altuck Evidence X-Powered-By: PHP/s.6.40-38+ubuniu20.04.1-deb.sury.org+1	URL	http://testphp.vulnweb.com/guestbook.php
Attack Evidence X-Powered By: PHP/5.6.40-38+ubuniu20.04.1+deb.sury.org+1 URL http://lestpha.vulnweb.com/hop/ Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuniu20.04.1+deb.sury.org+1 URL http://lestpha.vulnweb.com/hop/?ge=12 Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuniu20.04.1+deb.sury.org+1 Other Info URL http://lestpha.vulnweb.com/hop/?ge=12 Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuniu20.04.1+deb.sury.org+1 Other Info URL http://lestpha.vulnweb.com/hop/params.php?g=valid&pp=12 Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuniu20.04.1+deb.sury.org+1 Other Info URL http://lestpha.vulnweb.com/hop/params.php?g=valid&pp=12 Other Info URL http://lestpha.vulnweb.com/hop/params=1 Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuniu20.04.1+deb.sury.org+1 Other Info URL http://lestpha.vulnweb.com/hop/params=1 Method GET Parameter	Method	GET
Evidence X-Powered By: PHPIs.6.40-38+ubuntu20.04.1+deb.sury.org+1 URL httn://westphp.vu/moeb.com/npg/ Method GET Parameter Attack Evidence X-Powered-By: PHPIs.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL http://westphp.vu/moeb.com/npg/?gp=12 Method GET Parameter Attack Evidence X-Powered-By: PHPIs.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL http://westphp.vu/moeb.com/npg/?gp=12 Method GET URL http://westphp.vu/moeb.com/npg/?gp=12 Method GET Parameter Attack Evidence X-Powered-By: PHPIs.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL http://westphp.vu/moeb.com/npg/params.php?a-valid&pp=12 Method GET Parameter Attack Evidence X-Powered-By: PHPIs.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL http://westphp.vu/moeb.com/index.pbp Method GET Parameter Attack Evidence X-Powered-By: PHPIs.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL http://westphp.vu/moeb.com/index.pbp Method GET Parameter Attack Evidence X-Powered-By: PHPIs.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL http://westphp.vu/moeb.com/index.pbp Attack Evidence X-Powered-By: PHPIs.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info	Parameter	
Other Info URL http://testrpho.vulnweb.com/hgp/ Method GET Parameter Attack Evidence X-Powered-By. PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL http://testrpho.vulnweb.com/hgp/2gs=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://testpho.vulnweb.com/hpp/params.phb?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://testpho.vulnweb.com/hpp/params.phb?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://testpho.vulnweb.com/index.obp Method GET Parameter Attack Evidence X-Powered-By. PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL http://testpho.vulnweb.com/index.obp CET Parameter Attack Evidence X-Powered-By. PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL http://testpho.vulnweb.com/istarroducts.php?arfist=1 Method GET Parameter	Attack	
URL http://lestable.out/inveb.com/legi/ Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info Intip://lestable.out/inveb.com/legi/2pg=12 Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info Other Info URL http://lestable.out/inveb.com/lopi/params.php?p-valid&pg=12 Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 URL http://lestable.out/inveb.com/index.objp Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL Method GET Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL http://lestable.out/inveb.com/listarcolucts.php?artist=1 URL http://lestable.out/inveb.com/listarcolucts.php?artist=1	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL bttp://lestphp.vulnweb.com/bgp/2gg=12 Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL bttp://lestphp.vulnweb.com/bgp/params.php/2gs=42 Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL bttp://lestphp.vulnweb.com/bgp/params.php/2gs-valid8pg=12 Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL bttp://lestphp.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 bttp://lestphp.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 bttp://lestphp.vulnweb.com/index.php	Other Info	
Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu/20.04.1+deb.sury.org+1 URL http://testphp.vulnweb.com/hgq/?gg=12 Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu/20.04.1+deb.sury.org+1 Other Info URL http://testphp.vulnweb.com/hgp/params.php?p=valid&pp=12 Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu/20.04.1+deb.sury.org+1 Other Info URL http://testphp.vulnweb.com/hgp/params.php?p=valid&pp=12 Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu/20.04.1+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+ubuntu/20.04.1+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+ubuntu/20.04.1+deb.sury.org+1 Other Info URL http://testphp.vulnweb.com/listproducts.php?artist=1 Method GET Parameter	URL	http://testphp.vulnweb.com/hpp/
Attack Evidence	Method	GET
Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info Into://restphp.vulnweb.com/hpp/2pp=12 Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info Into://testphp.vulnweb.com/hpp/params.php?g=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 Intp://testphp.vulnweb.com/index.php URL http://testphp.vulnweb.com/index.php 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 Other Info URL http://testphp.vulnweb.com/listproducts.php?artist=1 Method GET Parameter	Parameter	
Other Info URL http://testphp.vulnweb.com/hpp/2np=12 Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04,1+deb.sury.org+1 Other Info 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 Method GET Parameter Attack Attack CET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL Other Info URL Method GET Parameter Attack Parameter Attack	Attack	
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.oho?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/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/index.php 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	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL Method GET Parameter Attack Attack Set T 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 Method GET	Other Info	
Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL http://testphp.xulnweb.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.xulnweb.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.xulnweb.com/index.php Other Info URL http://testphp.xulnweb.com/index.php Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL http://testphp.xulnweb.com/listproducts.php?artist=1 Method GET Parameter	URL	http://testphp.vulnweb.com/hpp/?pp=12
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/index.php Method GET Other Info URL http://testphp.vulnweb.com/listproducts.php?arriist=1 Method GET Parameter	Method	GET
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/index.php Other Info URL http://testphp.vulnweb.com/istproducts.php?artist=1 Method GET Parameter Method GET Parameter	Parameter	
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/index.php Other Info URL 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	Attack	
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 Method GET Parameter Attack Evidence X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 Other Info URL URL http://testphp.vulnweb.com/listproducts.php?artist=1 Method GET Parameter http://testphp.vulnweb.com/listproducts.php?artist=1 Method GET	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+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/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 Mttp://testphp.vulnweb.com/listproducts.php?artist=1 Method GET Parameter	Other Info	
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	URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
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	Method	GET
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	Parameter	
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	
URL http://testphp.vulnweb.com/index.php Method GET Parameter	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+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=1 Method GET Parameter	Other Info	
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	URL	http://testphp.vulnweb.com/index.php
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	Method	GET
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	Parameter	
Other Info URL http://testphp.vulnweb.com/listproducts.php?artist=1 Method GET Parameter	Attack	
URL http://testphp.vulnweb.com/listproducts.php?artist=1 Method GET Parameter Value of the product of the produc	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Method GET Parameter	Other Info	
Parameter	URL	http://testphp.vulnweb.com/listproducts.php?artist=1
	Method	GET
Attack	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	

Е	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
N	Method	GET
Р	Parameter	
А	Attack	
Е	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
0	Other Info	
URL		http://testphp.vulnweb.com/product.php?pic=4
N	Method	GET
Р	Parameter	
А	Attack	
Е	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
0	Other Info	
URL		http://testphp.vulnweb.com/product.php?pic=5
N	Method	GET
Р	Parameter	
А	Attack	
E	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
0	Other Info	
URL		http://testphp.vulnweb.com/product.php?pic=6
N	Method	GET
Р	Parameter	
А	Attack	
Е	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
0	Other Info	
URL	-	http://testphp.vulnweb.com/product.php?pic=7
N	Method	GET
Р	Parameter	
А	Attack	
Е	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
0	Other Info	
URL	-	http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'
N	Method	GET
Р	Parameter	
А	Attack	
E	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
0	Other Info	
URL		http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
	Method	GET
N	vietriou	OE1

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	
1	

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
0.12	
Method	POST
Method	
Method Parameter	
Method Parameter Attack	POST
Method Parameter Attack Evidence	POST X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Method Parameter Attack Evidence Other Info	POST

Parameter	
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
Instances	62
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08- <u>Fingerprint_Web_Application_Framework</u> https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	<u>497</u>
WASC Id	13
Plugin Id	<u>10037</u>
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	
Request Header	GET http://testphp.vulnweb.com/ HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/5 37.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 0K Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:12 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 4958
Response Body (truncated)	<pre><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false"--> <head> <meta content="text/html; charset=utf-8" http-equiv="Content-Type"/> <!-- InstanceBeginEditable name="document_title_rgn"--> <title>Home of Acunetix Art</title> <!-- InstanceEndEditable--> <!-- InstanceEndEditable--> <!-- InstanceBeginEditable(truncated)</pre--></head></html></pre>

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/favicon.ico
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	
		nginx/1.19.0
	Other Info	
UR		http://testphp.vulnweb.com/hpp/?pp=12
	Method	GET
	Parameter	
	Attack	
		nginx/1.19.0
	Other Info	
UR	RL.	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
	Method	GET
	Parameter	
	Attack	
	Evidence	nginx/1.19.0
	Other Info	
UR	Ł	http://testphp.vulnweb.com/images/logo.gif
	Method	GET
	Parameter	
	Attack	
	Evidence	nginx/1.19.0
	Other Info	
UR	łL	http://testphp.vulnweb.com/images/remark.gif
	Method	GET
	Parameter	
	Attack	
	Evidence	nginx/1.19.0
	Other Info	
UR	!L	http://testphp.vulnweb.com/index.php
	Method	GET
	Parameter	
	Attack	
		nginx/1.19.0
	Other Info	
UR		http://testphp.vulnweb.com/listproducts.php?artist=1
	Method	GET
	Parameter	
	Attack	
		nginx/1.19.0
	Other Info	
i		

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

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/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	
	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
Method	GET
Parameter	
Attack	
	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg
Method	GET
Parameter	
Attack	
	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	75
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	<u>497</u>
WASC Id	13
Plugin Id	<u>10036</u>
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.
Request Header	GET http://testphp.vulnweb.com/ HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/5 37.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 0K Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:12 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 4958

Response Body (truncated)	<pre><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> </pre>
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	

Method GET Attack Method GET Attack Evidence Other Info Method GET Attack Evidence Other Info Method GET Attack Evidence Other Info Method GET Parameter **content-type-options Attack Evidence Method GET Attack Evidence Other Info Other Info Method GET Attack Evidence Other Info Other Info Other Info Method GET Attack Evidence Other Info Other Info Other Info Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the page is the p	
Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for type larges (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for type larges (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for type larges (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for type larges (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for type pages (401, 403, 500, etc.) a	
Attack Evidence Other Info Other	
Evidence Other Info Ot	
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 lafe This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the parameter and the page is a still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the page are often still affected by	
browsers 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 Arcontent-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 Arcontent-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the content type applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the content type applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the content type applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the content type applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the content type applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the content type applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the content type applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is	
Method GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still concern for the pages are often still affected by injection issues, in which case there is still affected by injec)r
Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 the pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the pages (401, 403, 500, etc.) as the pages (401, 403, 500, etc.	or
Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still affected by injection issues, in which case there is still affected by injection issues, in which case there is still affected by injection issues, in which case there is still affected by injection issues, in which case there is still affected by injection issues, in which case there is still	or
Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues.	or
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues, in which case there is still concern for the still affected by injection issues.	or
browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. Line	or
Method GET Parameter x-content-type-options Attack Evidence Other lefe This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still applies to error type pages (401, 403, 500, etc.)	
Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern f	
Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern f	
Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for the still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still applies to error type pages (401, 403, 500, etc.) as the still applies to error type pages (401, 403, 500, etc.) as the still applies to error type pages (401, 403, 500, etc.) as the still applies to error type pages (401, 403, 500, etc.) as the still applies to error type pages (401, 403, 500, etc.) as the still applies to error type pages (401, 403, 500, etc.) as the still applies to error type pages (401, 403, 500, etc.) as the still applies to error type pages (401, 403, 500, etc.) as the still applies to error type pages (401, 403, 500, etc.) as the still applies to error type pages (401, 403, 500, etc.) as the still applies to error type pages (401, 403, 500, etc.) as the still applies to error type pages (401, 403, 6	
Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern f	
	or
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 f browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.	or
URL http://testphp.vulnweb.com/favicon.ico	
Method GET	
Parameter x-content-type-options	
Attack	
Evidence	
Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.	r
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/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/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	

URL http://westplip.vulnweb.com/product.php?pic=S Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are other still affected by injection issues, in which case there is still concern for browsers infining pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. Info Other Info Othe	Method GET Parameter Cheer info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concein type. At Tright his school this scan rule will not alert on client or server error responses. URL Inter-Missiento-vulnwish-comfunction fulls/Pased Method OET Parameter Accontant-type-applions Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concein type. At Tright threshold this scan rule will not alert on client or server error responses. URL Inter-Missiento-vulnwish-comfunction pages away from their aduat content type, At Tright threshold this scan rule will not alert on client or server error responses. URL Method GET Parameter Accontent-type-applions Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concein the provinces a stilling pages away from their actual content type. At Tright threshold this scan rule will not alert on client or server error responses. URL Inter-Missiento-vulnwest-comfunction into Pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concein the provinces a stilling pages away from their actual content type. At Tright threshold this scan rule will not alert on client or server error responses. URL Inter-Missiento-vulnwest-comfunction into Pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still conceined to page and the page are often still affected by injection issues, in which case there is still conceined to page and page away from their actual content type. At Tright threshold this scan rule will not alert on client or server error responses. URL Method GET Parameter Actual Actu	Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Parameter xcontent-type-options Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers suffling pages away from their actual content type. Al "High" threshold this scan rule will not alert on client or server error responses. URL Method GET Parameter x-content-type-options Attack Evidence Other Info Orives in Sill applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers suffling pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://inscipho.com/product.pho/pic=5 Method GET Parameter x-content-type-options Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers suffling pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://iessipho.goulinveb.com/product.pho/pic=5 Other Info GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers suffling pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://iessipho.goulinveb.com/product.pho/pic=5 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers soffling pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://iessipho.goul	Parameter Attack Evidence Other Info Other	URL	http://testphp.vulnweb.com/product.php?pic=3
Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL Method GET Parameter **content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL **Method GET Parameter **content-type-options Attack Evidence Other Info Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL **http://hestoth.put.inveb.com/product.php?pic=5 Wethod GET Parameter **content-type-options This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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://hestoth.put.inveb.com/product.php?pic=5 Method GET Parameter **Content-type-options This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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://hestoth.put.nueb.com/product.php?pic=5	Attack Evidence Other Info O	Method	GET
Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL Method GET Parameter Actack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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.ptp?pic=5 Method GET Parameter Actack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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.ptp?pic=6 Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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.ptp?pic=6 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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.ptp?pic=6 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affecte	Evidence Other Info Other In	Parameter	x-content-type-options
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers smifting pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. Method GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers smifting pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL Method GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers smifting pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL Into the info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers smifting pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL Method GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers smifting 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is	Other Info brivases still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concerned. URL http://stspip.vulmveb.com/product.php?pic=4 Method GET Parameter x-content-type-options Attack Evidence Other Info brivases stilling pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL btto://westphp.vulmveb.com/product.php?pic=5 GET Parameter x-content-type-options Attack Evidence Other Info brivases stilling pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. Method GET Parameter x-content-type-options Attack Evidence Other Info brivases stilling pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL bttp://westphp.vulmveb.com/product.php?pic=6 Other Info brivases stilling pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL bttp://westphp.vulmveb.com/product.php?pic=6 Method GET Parameter x-content-type options Attack Evidence Other Info brivases stilling pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL bttp://westphp.vulmveb.com/product.php?pic=7 Method GET Parameter x-content-type-options Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still conc browsers smilling pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL bttp://westphp.vulmveb.com/product.php?pic=7 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case the	Attack	
URL http://estohp.vulnweb.com/product.php?pic=4 Method GET Parameter x-content-type-options Attack Evidence Other Info Other Info OGET Parameter x-content-type-options Attack Evidence Other Info Other Info Other Info OGET Parameter x-content-type-options Attack Evidence Other Info Other Info Other Info OGET Parameter x-content-type-options Attack Evidence Other Info Other Info Other Info OGET Parameter x-content-type-options Attack Evidence Other Info Other Info OGET Parameter x-content-type-options Attack Evidence Other Info	URL http://testph.vulnweb.com/product.phg?pic=4 Method GET Parameter x-content-type-options Attack Evidence Other Info Method GET Parameter x-content-type-options Attack Evidence Other Info Intrinsia issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concentrate type. At "High" threshold this stan rule will not allert on client or server error responses. URL http://testph.vulnweb.com/product.phg?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 concentrate type. At "High" threshold this stan rule will not allert on client or server error responses. URL http://testph.vulnweb.com/product.phg?pic=6 Other Info Other Info GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concentrate type. At "High" threshold this scan rule will not allert on client or server error responses. URL http://testph.vulnweb.com/product.phg?pic=6 CET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concentrate type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testph.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 concentrate type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testph.	Evidence	
Method GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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://testpho.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://testpho.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://testpho.vulnweb.com/product.php?pic=7 Wethod GET Parameter x-content-type-options Attack Method GET Parameter x-content-type-options	Method GET Parameter	Other Info	
Parameter x-content-type-options Attack Evidence Other Into This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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?gic=5 Method GET Parameter x-content-type-options Attack Evidence Other Into browsers 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?gic=6 Method GET Parameter x-content-type-options Attack Evidence Other Into This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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	Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concluded. http://discripty.vulnweb.com/product.php?qic=5 Wethod GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concluded the providence of the providenc	URL	http://testphp.vulnweb.com/product.php?pic=4
Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL Method GET Parameter A-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 GET Parameter Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 GET Parameter Accontent-type-options	Attack Evidence Other Info Other	Method	GET
Evidence Other Info Ot	Evidence Other Info Other In	Parameter	x-content-type-options
This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. Method GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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	Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concording to browsers on http://teshpho.vulnweb.com/product.php?pic=5 Method GET Parameter Accontent-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concording to the conc	Attack	
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 Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 Note http://testphp.vulnweb.com/product.php?pic=7 Method GET Parameter x-content-type-options Attack	URL http://testphp.vulnweb.com/product.php?pic=5 Method GET Parameter x-content-type-options Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concombrowsers 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 Attack Evidence GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concombrowed the product page of the	Evidence	
Method GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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	Method GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concorder type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/product.phg?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 concorder type in the interview of the i	Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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	Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concording 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 concording the pages are often still affected by injection issues, in which case there is still concording the pages are often still affected by injection issues, in which case there is still concording the pages are often still affected by injection issues, in which case there is still concording the pages are often still affected by injection issues, in which case there is still concording the pages are often still affected by injection issues, in which case there is still concording the pages are often still affected by injection issues, in which case there is still concording the pages are often still affected by injection issues, in which case there is still concording the pages are often still affected by injection issues, in which case there is still concording the pages are often still affected by injection issues, in which case there is still concording the pages are often still affected by injection issues, in which case there is still concording the pages are often still affected by injection issues, in which case there is still concording the pages are often still affected by injection issues, in which case there is still concording the pages are often still affected by injection issues, in which case there is still concording the pages are often still affected by injection issues, in which case there is still concording the pages are often still affected by injection iss	URL	http://testphp.vulnweb.com/product.php?pic=5
Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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	Attack Evidence Other Info Dither Info GET Parameter Accontent-type-options Attack Evidence Other Info Dither Inf	Method	GET
Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by injection issues, in which case there is still concorded by the provided by the provid	Parameter	x-content-type-options
Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. INCL http://testphp.vulnweb.com/product.php?pic=6 GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concord browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. INTL Method GET Parameter Accentent-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concord browsers 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 Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concord the concording to the conc	Attack	
browsers 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	DURL Attack Evidence Other Info Other I	Evidence	
Method GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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	Method GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still conconducted by the pages and the page of the pages and the page of the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affected by injection issues, in which case there is still conconducted by the pages are often still affe	Other Info	
Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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	Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concord browsers 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 concord browsers 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	URL	http://testphp.vulnweb.com/product.php?pic=6
Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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	Attack Evidence Other Info Other	Method	GET
Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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 Other Info Other Info Other Info Other Info Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still conconduct. URL http://testphp.vulnweb.com/product.php?pic=7 Method GET Parameter Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still conconduct 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	Parameter	x-content-type-options
Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concord browsers 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 Arameter Accontent-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concord browsers 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	
browsers 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	browsers 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 concord browsers 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	Evidence	
Method GET Parameter x-content-type-options Attack	Method GET Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still conc browsers 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	Other Info	
Parameter x-content-type-options Attack	Parameter x-content-type-options Attack Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still conc browsers 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	URL	http://testphp.vulnweb.com/product.php?pic=7
Attack	Attack Evidence Other Info Other Info URL http://testphp.vulnweb.com/secured/style.css Method GET Parameter Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still conc browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. Method GET Parameter x-content-type-options	Method	GET
	Evidence Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still conc browsers 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	Parameter	x-content-type-options
Evidence	Other Info Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still conc browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. INCL Method GET Parameter Arcontent-type-options	Attack	
	browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL Method GET Parameter x-content-type-options	Evidence	
Other Info This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.	Method GET Parameter x-content-type-options	Other Info	
URL http://testphp.vulnweb.com/secured/style.css	Parameter x-content-type-options	URL	http://testphp.vulnweb.com/secured/style.css
Method GET		Method	GET
Parameter x-content-type-options		Parameter	x-content-type-options
Attack	Attack	Attack	
Evidence	Evidence	Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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	

URL Method Parameter Attack Evidence	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160 GET x-content-type-options
Parameter Attack	x-content-type-options
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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	
Parameter Attack	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers 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	69
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.
Reference	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	<u>693</u>
WASC Id	15
Plugin Id	<u>10021</u>
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

userParam=uemail userValue=ZAP passwordParam=upass referer=http://testphp.vulnweb.com/signup.php

Attack Evidence

Other Info

upass

Request Header	POST http://testphp.vulnweb.com/secured/newuser.php HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/5 37.36 pragma: no-cache cache-control: no-cache cache-control: no-cache content-type: application/x-www-form-urlencoded referer: http://testphp.vulnweb.com/signup.php content-length: 96
Request Body	uuname=ZAP&upass=ZAP&upass2=ZAP&urname=ZAP&ucc=ZAP&uemail=ZAP&uphone=ZAP&uaddress=&signup=signup
Response Header	HTTP/1.1 200 0K Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:13 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 733
Response Body (truncated)	<pre><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> </pre>
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.
Request Header	GET http://testphp.vulnweb.com/ HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/5 37.36 pragma: no-cache cache-control: no-cache
Request Body	
Response Header	HTTP/1.1 200 OK Server: nginx/1.19.0 Date: Tue, 23 Sep 2025 22:46:12 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 content-length: 4958
Response Body (truncated)	<pre><!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd"> <html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false"--> <head> <meta content="text/html; charset=utf-8" http-equiv="Content-Type"/> <!-- InstanceBeginEditable name="document_title_rgn"--> <title>Home of Acunetix Art</title> <!-- InstanceEndEditable--> <ink href="style.css" rel="stylesheet" type="text/css"> <!-- InstanceBeginEditable(truncated)</pre--></ink></head></html></pre>
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/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	31
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id	<u>436</u>
WASC Id	15
Plugin Id	90011
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
Request Header	POST http://testphp.vulnweb.com/guestbook.php HTTP/1.1 host: testphp.vulnweb.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/5 37.36 pragma: no-cache cache-control: no-cache cache-control: no-cache content-type: application/x-www-form-urlencoded referer: http://testphp.vulnweb.com/guestbook.php content-length: 33
Request Body	name=ZAP&text=&submit=add+message

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	<u>20</u>
WASC Id	20
Plugin Id	<u>10031</u>