ZAP by Checkmarx Scanning Report

Site: http://testphp.vulnweb.com

Generated on Thu, 20 Feb 2025 01:00:05

ZAP Version: 2.16.0

ZAP by Checkmarx

Summary of Alerts

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

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	4
Content Security Policy (CSP) Header Not Set	Medium	51
Missing Anti-clickjacking Header	Medium	44
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	71
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	84
X-Content-Type-Options Header Missing	Low	75
Authentication Request Identified	Informational	1
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	30
Information Disclosure - Suspicious Comments	Informational	1
Modern Web Application	Informational	9
User Controllable HTML Element Attribute (Potential XSS)	Informational	4

Alert Detail

Medium	Absence of Anti-CSRF Tokens
	No Anti-CSRF tokens were found in a HTML submission form.

Description	A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL /form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.
	CSRF attacks are effective in a number of situations, including:
	* The victim has an active session on the target site.
	* The victim is authenticated via HTTP auth on the target site.
	* The victim is on the same local network as the target site.
	CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	
Evidence	<form action="" method="post" name="faddentry">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "name" "submit"].
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Attack	
Evidence	<form action="search.php?test=query" method="post">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"].

Instances	4
Solution	Phase: Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Implementation

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.

This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

Phase: Implementation

Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons. |
| Reference | https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html
https://cwe.mitre.org/data/definitions/352.html |
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	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/AJAX/index.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/artists.php

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

	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/comment.php?aid=3
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/disclaimer.php
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/guestbook.php
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/high
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/hpp/
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/hpp/?pp=12
	Method	GET
	Attack	
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12
	Method	GET
	Attack	
	Evidence	

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

URL	http://testphp.vulnweb.com/listproducts.php?cat=4		
Method	GET		
Attack			
Evidence			
Other Info			
URL	http://testphp.vulnweb.com/login.php		
Method	GET		
Attack			
Evidence			
Other Info			
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/		
Method	GET		
Attack			
Evidence			
Other Info			
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/		
Method	GET		
Attack			
Evidence			
Other Info			
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/		
Method	GET		
Attack			
Evidence			
Other Info			
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/		
Method	GET		
Attack			
Evidence			
Other Info			
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/		
Method	GET		
Attack			
Evidence			
Other Info			
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/		
Method	GET		

Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2/	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/privacy.php	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/product.php?pic=1	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/product.php?pic=2	
Method	GET	
Attack		

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

Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX/showxml.php
Method	POST
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Attack	
Evidence	
Other Info	
Instances	51
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP /Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/

	https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

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

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

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

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

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

URL	http://testphp.vulnweb.com/product.php?pic=5
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=6
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=7
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/signup.php
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX/showxml.php
Method	POST
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST

Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Attack	
Evidence	
Other Info	
Instances	44
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.

If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive. |
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

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

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

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

Other Info		
URL	http://testphp.vulnweb.com/hpp/	
Method	GET	
Attack		
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1	
Other Info		
URL	http://testphp.vulnweb.com/hpp/?pp=12	
Method	GET	
Attack		
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1	
Other Info		
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12	
Method	GET	
Attack		
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1	
Other Info		
URL	http://testphp.vulnweb.com/index.php	
Method	GET	
Attack		
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1	
Other Info		
URL	http://testphp.vulnweb.com/listproducts.php?artist=1	
Method	GET	
Attack		
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1	
Other Info		
URL	http://testphp.vulnweb.com/listproducts.php?artist=2	
Method	GET	
Attack		
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1	
Other Info		
URL	http://testphp.vulnweb.com/listproducts.php?artist=3	
Method	GET	
Attack		
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1	
Other Info		

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

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

	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
URL		http://testphp.vulnweb.com/privacy.php
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
URL		http://testphp.vulnweb.com/product.php?pic=1
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
URL		http://testphp.vulnweb.com/product.php?pic=2
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
URL		http://testphp.vulnweb.com/product.php?pic=3
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
URL		http://testphp.vulnweb.com/product.php?pic=4
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
URL		http://testphp.vulnweb.com/product.php?pic=5
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
URL		http://testphp.vulnweb.com/product.php?pic=6
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other	

	Info	
	URL	http://testphp.vulnweb.com/product.php?pic=7
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
	URL	http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
	URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
	URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
	URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
	URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
	URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
	Method	GET
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	

URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&size=160
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg
Method	GET

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

	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
URL		http://testphp.vulnweb.com/secured/newuser.php
	Method	POST
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
URL		http://testphp.vulnweb.com/userinfo.php
	Method	POST
	Attack	
	Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
	Other Info	
Instances		71
Solution		Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference		https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
CWE Id		200
WASC Id		13
Plugin Id		10037

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

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

	URL	http://testphp.vulnweb.com/artists.php?artist=2
	Method	GET
	Attack	
	Evidence	nginx/1.19.0
	Other Info	
	URL	http://testphp.vulnweb.com/artists.php?artist=3
	Method	GET
	Attack	
	Evidence	nginx/1.19.0
	Other Info	
	URL	http://testphp.vulnweb.com/cart.php
	Method	GET
	Attack	
	Evidence	nginx/1.19.0
	Other Info	
	URL	http://testphp.vulnweb.com/categories.php
	Method	GET
	Attack	
	Evidence	nginx/1.19.0
	Other Info	
	URL	http://testphp.vulnweb.com/comment.php?aid=1
	Method	GET
	Attack	
	Evidence	nginx/1.19.0
	Other Info	
	URL	http://testphp.vulnweb.com/comment.php?aid=2
	Method	GET
	Attack	
	Evidence	nginx/1.19.0
	Other Info	
	URL	http://testphp.vulnweb.com/comment.php?aid=3
	Method	GET
	Attack	
	Evidence	nginx/1.19.0
	Other Info	
	URL	http://testphp.vulnweb.com/disclaimer.php
	Method	GET

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

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

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

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

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

Other Info		
URL	http://testphp.vulnweb.com/product.php?pic=5	
Method	GET	
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/product.php?pic=6	
Method	GET	
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/product.php?pic=7	
Method	GET	
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/robots.txt	
Method	GET	
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/secured/style.css	
Method	GET	
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20'	
Method	GET	
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg	
Method	GET	
Attack		
Evidence	nginx/1.19.0	
Other		

Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg

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

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

Other Info		
URL	http://testphp.vulnweb.com/userinfo.php	
Method	POST	
Attack		
Evidence	nginx/1.19.0	
Other Info		
Instances	84	
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	200	
WASC Id	13	
Plugin Id	10036	

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

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

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

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

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

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

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

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

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.	
URL	http://testphp.vulnweb.com/product.php?pic=2	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.	
URL	http://testphp.vulnweb.com/product.php?pic=3	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.	
URL	http://testphp.vulnweb.com/product.php?pic=4	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.	
URL	http://testphp.vulnweb.com/product.php?pic=5	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.	
URL	http://testphp.vulnweb.com/product.php?pic=6	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.	
URL	http://testphp.vulnweb.com/product.php?pic=7	
Method	GET	
Attack		
Evidence		
	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still	

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

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

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

	or server error responses.
URL	http://testphp.vulnweb.com/AJAX/showxml.php
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/cart.php
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/search.php?test=query
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	75
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing. |
| Reference | https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) |

	https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	Authentication Request Identified
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Attack	
Evidence	upass
Other Info	userParam=uemail userValue=ZAP passwordParam=upass referer=http://testphp.vulnweb.com/signup.php
Instances	1
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

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

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

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

Method	GET	
Attack		
Evidence		
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.	
URL	http://testphp.vulnweb.com/product.php?pic=1	
Method	GET	
Attack		
Evidence		
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.	
URL	http://testphp.vulnweb.com/product.php?pic=2	
Method	GET	
Attack		
Evidence		
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.	
URL	http://testphp.vulnweb.com/product.php?pic=3	
Method	GET	
Attack		
Evidence		
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.	
URL	http://testphp.vulnweb.com/product.php?pic=4	
Method	GET	
Attack		
Evidence		
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.	
URL	http://testphp.vulnweb.com/product.php?pic=5	
Method	GET	
Attack		
Evidence		
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.	
URL	http://testphp.vulnweb.com/product.php?pic=6	
Method	GET	
Attack		
Evidence		
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.	
URL	http://testphp.vulnweb.com/product.php?pic=7	
Method	GET	

Attack		
Evidence		
Other Info		There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL		http://testphp.vulnweb.com/signup.php
Method		GET
Attack		
Evidence		
Other Info		There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL		http://testphp.vulnweb.com/cart.php
Method		POST
Attack		
Evidence		
Other Info		There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL		http://testphp.vulnweb.com/guestbook.php
Method		POST
Attack		
Evidence		
Other Info		There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL		http://testphp.vulnweb.com/search.php?test=query
Method		POST
Attack		
Evidence		
Other Info		There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL		http://testphp.vulnweb.com/secured/newuser.php
Method		POST
Attack		
Evidence		
Other Info		There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-1] do not match.
Instances		30
Solution		Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference		https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id		436
WASC Id		15
Plugin Id		90011

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

	URL	http://testphp.vulnweb.com/AJAX/index.php
	Method	GET
	Attack	
	Evidence	where
	Other Info	The following pattern was used: \bWHERE\b and was detected in the element starting with: "<script type="text/javascript"> var httpreq = null; function SetContent(XML) { var items = XML.getElementsByTagName('i", see evidence field for the suspicious comment/snippet.
Instances		1
Solution		Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference		
CWE Id		200
WASC Id		13
Plugin Id		10027

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

Attack	
Evidence	`<a href='#' onClick="window.open('./comment.php?aid=3','comment','width=500, height=400')">comment on this artist</a>`
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?artist=1
Method	GET
Attack	
Evidence	`<a href='#' onClick="window.open('./comment.php?pid=1','comment','width=500, height=400')">comment on this picture</a>`
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?artist=2
Method	GET
Attack	
Evidence	`<a href='#' onClick="window.open('./comment.php?pid=7','comment','width=500, height=400')">comment on this picture</a>`
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?cat=1
Method	GET
Attack	
Evidence	`<a href='#' onClick="window.open('./comment.php?pid=1','comment','width=500, height=400')">comment on this picture</a>`
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/listproducts.php?cat=2
Method	GET
Attack	
Evidence	`<a href='#' onClick="window.open('./comment.php?pid=6','comment','width=500, height=400')">comment on this picture</a>`
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Instances	9
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	User Controllable HTML Element Attribute (Potential XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST

Attack		
Evidence		
Other Info		User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://testphp.vulnweb.com /guestbook.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: name=anonymous user The user-controlled value was: anonymous user
URL		http://testphp.vulnweb.com/guestbook.php
Method		POST
Attack		
Evidence		
Other Info		User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://testphp.vulnweb.com /guestbook.php appears to include user input in: a(n) [input] tag [value] attribute The user input found was: submit=add message The user-controlled value was: add message
URL		http://testphp.vulnweb.com/search.php?test=query
Method		POST
Attack		
Evidence		
Other Info		User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://testphp.vulnweb.com/search. php?test=query appears to include user input in: a(n) [input] tag [name] attribute The user input found was: goButton=go The user-controlled value was: gobutton
URL		http://testphp.vulnweb.com/search.php?test=query
Method		POST
Attack		
Evidence		
Other Info		User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://testphp.vulnweb.com/search. php?test=query appears to include user input in: a(n) [input] tag [value] attribute The user input found was: goButton=go The user-controlled value was: go
Instances	4	
Solution	Validate all input and sanitize output it before writing to any HTML attributes.	
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html	
CWE Id	20	
WASC Id	20	
Plugin Id	10031	