ZAP ScanAtivo

Sites: http://clients2.google.com http://testphp.vulnweb.com

Generated on Mon, 29 Sept 2025 18:16:02

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	3
Medium	6
Low	3
Informational	6

Alerts

Name	Risk Level	Number of Instances
Cross Site Scripting (DOM Based)	High	13
Cross Site Scripting (Reflected)	High	20
SQL Injection - MySQL	High	16
Absence of Anti-CSRF Tokens	Medium	42
Application Error Disclosure	Medium	1
Content Security Policy (CSP) Header Not Set	Medium	71
Directory Browsing	Medium	3
Missing Anti-clickjacking Header	Medium	53
XSLT Injection	Medium	1
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	84
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	118
X-Content-Type-Options Header Missing	Low	91
Authentication Request Identified	Informational	3
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	35
GET for POST	Informational	3
Modern Web Application	Informational	10
User Agent Fuzzer	Informational	218
User Controllable HTML Element Attribute (Potential XSS)	Informational	4

Alert Detail

High	Cross Site Scripting (DOM Based)
Description	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML /JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology. When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise. There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash. Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code.
URL	http://testphp.vulnweb.com#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Method	GET
Attack	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[1] Access: http://testphp.vulnweb.com<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[2] Access: http://testphp.vulnweb.com<PAYLOAD_0>
URL	http://testphp.vulnweb.com/#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Method	GET
Attack	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/<

Other Info	/teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/<PAYLOAD_0>
URL	http://testphp.vulnweb.com/artists.php?artist=3#jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Method	GET
Attack	#jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/artists.php?artist=3<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/artists.php?artist=3<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/artists.php?artist=3<PAYLOAD_0>
URL	http://testphp.vulnweb.com/cart.php#jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Method	GET
Attack	#jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/cart.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/cart.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/cart.php<PAYLOAD_0> Click element: /html/body/div[1]
URL	http://testphp.vulnweb.com/categories.php#jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Method	GET
Attack	#jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/categories.php<PAYLOAD_0> Write to /html/body/div[1]/div[8]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[8]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/categories.php<PAYLOAD_0> Write to /html/body/div[1]/div[8]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[8]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/categories.php<PAYLOAD_0>
URL	http://testphp.vulnweb.com/disclaimer.php#jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Method	GET

Attack	#jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e	
Evidence		
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/disclaimer.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/disclaimer.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/disclaimer.php<PAYLOAD_0> Click element: /html/body/div[1] Access: http://testphp.vulnweb.com/disclaimer.php<PAYLOAD_0> Click element: /html/body/div[1]/div[1] Access: http://testphp.vulnweb.com/disclaimer.php<PAYLOAD_0>	
URL	http://testphp.vulnweb.com/guestbook.php#jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e	
Method	GET	
Attack	#jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e	
Evidence		
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div[2]/form/input[1] the value: <PAYLOAD_0> Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div[2]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[3]/div[2]/form/input[2] Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0> Write to /html/body/div[1]/div[6]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[6]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0> Write to /html/body/div[1]/div[6]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[6]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0> Click element: /html/body/div[1] Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0> Click element: /html/body/div[1]/div[1] Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0>	
URL	http://testphp.vulnweb.com/hpp/params.php?p=%3Cscript%3Ealert(5397)%3C/script%3E&pp=12	
Method	GET	
Attack	<script>alert(5397)</script>	
Evidence		
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_1> as: %3Cscript%3Ealert(5397)%3C/script%3E Access: http://testphp.vulnweb.com/hpp/params.php?p=<PAYLOAD_1>&pp=12	
URL	http://testphp.vulnweb.com/index.php#jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e	
Method	GET	
Attack	#jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e	
Evidence		
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/((/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/index.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/index.php<PAYLOAD_0> Write to /html/body/div[1]/div	

	[5]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/index.php<PAYLOAD_0>
URL	http://testphp.vulnweb.com/listproducts.php?cat=4#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Method	GET
Attack	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/listproducts.php?cat=4<PAYLOAD_0> Write to /html/body/div[1]/div[4]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[4]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/listproducts.php?cat=4<PAYLOAD_0> Write to /html/body/div[1]/div[4]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[4]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/listproducts.php?cat=4<PAYLOAD_0>
URL	http://testphp.vulnweb.com/cart.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Method	POST
Attack	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/cart.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/cart.php<PAYLOAD_0> Write to /html/body/div[1]/div[5]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[5]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/cart.php<PAYLOAD_0> Click element: /html/body/div[1] Access: http://testphp.vulnweb.com/cart.php<PAYLOAD_0>
URL	http://testphp.vulnweb.com/guestbook.php#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Method	POST
Attack	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div[2]/form/input[1] the value: <PAYLOAD_0> Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0> Write to /html/body/div[1]/div[3]/div[2]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[3]/div[2]/form/input[2] Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0> Write to /html/body/div[1]/div[6]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[6]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0> Write to /html/body/div[1]/div[6]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[6]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/guestbook.php<PAYLOAD_0>
URL	http://testphp.vulnweb.com/search.php?test=query#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Method	POST

Attack	#jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e
Evidence	
Other Info	The following steps were done to trigger the DOM XSS: With <PAYLOAD_0> as: #jaVasCript:/*-/*`/*\`/*'/*"/**/(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a//</stYle/</titLe/</teXtarEa/</scRipt/--!>\x3csVg/<sVg/oNloAd=alert(5397)//>\x3e Access: http://testphp.vulnweb.com/search.php?test=query<PAYLOAD_0> Write to /html/body/div[1]/div[4]/div[1]/form/input[1] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[4]/div[1]/form/input[1] Access: http://testphp.vulnweb.com/search.php?test=query<PAYLOAD_0> Write to /html/body/div[1]/div[4]/div[1]/form/input[2] the value: <PAYLOAD_0> Click element: /html/body/div[1]/div[4]/div[1]/form/input[2] Access: http://testphp.vulnweb.com/search.php?test=query<PAYLOAD_0>
Instances	13
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.

Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.

Phases: Implementation; Architecture and Design

Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.

For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters.

Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed.

Phase: Architecture and Design

For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.

If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.

Phase: Implementation

For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping.

To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set. |

	Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.
Reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Plugin Id	40026

High	Cross Site Scripting (Reflected)
Description	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML /JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or any other browser-supported technology. When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privilege, the code has the ability to read, modify and transmit any sensitive data accessible by the browser. A Cross-site Scripted user could have his/her account hijacked (cookie theft), their browser redirected to another location, or possibly shown fraudulent content delivered by the web site they are visiting. Cross-site Scripting attacks essentially compromise the trust relationship between a user and the web site. Applications utilizing browser object instances which load content from the file system may execute code under the local machine zone allowing for system compromise. There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack. Using a malicious form will oftentimes take place when the vulnerable resource only accepts HTTP POST requests. In such a case, the form can be submitted automatically, without the victim's knowledge (e.g. by using JavaScript). Upon clicking on the malicious link or submitting the malicious form, the XSS payload will get echoed back and will get interpreted by the user's browser and execute. Another technique to send almost arbitrary requests (GET and POST) is by using an embedded client, such as Adobe Flash. Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often include message board posts, web mail messages, and web chat software. The unsuspecting user is not required to interact with any additional site/link (e.g. an attacker site or a malicious link sent via email), just simply view the web page containing the code.
URL	http://testphp.vulnweb.com/artists.php?artist=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Method	GET
Attack	<scrIpt>alert(1);</scrIpt>

Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/hpp/?pp=%22+onMouseOver%3D%22alert%281%29%3B
Method	GET
Attack	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?p=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E&pp=12
Method	GET
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Method	GET
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?artist=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Method	GET
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/listproducts.php?cat=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Method	GET
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/product.php?pic=%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Method	GET
Attack	<scrIpt>alert(1);</scRipt>
Evidence	<scrIpt>alert(1);</scRipt>
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=%27%22%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
Method	GET

	Attack	'"<scrIpt>alert(1);</scRipt>
	Evidence	'"<scrIpt>alert(1);</scRipt>
	Other Info	
URL		http://testphp.vulnweb.com/guestbook.php
	Method	POST
	Attack	<scrIpt>alert(1);</scRipt>
	Evidence	<scrIpt>alert(1);</scRipt><strong>
	Other Info	
URL		http://testphp.vulnweb.com/guestbook.php
	Method	POST
	Attack	</td><scrIpt>alert(1);</scRipt><td>
	Evidence	</td><scrIpt>alert(1);</scRipt><td>
	Other Info	
URL		http://testphp.vulnweb.com/search.php?test=%27%22%3CscrIpt%3Ealert%281%29%3B%3C%2FscRipt%3E
	Method	POST
	Attack	'"<scrIpt>alert(1);</scRipt>
	Evidence	'"<scrIpt>alert(1);</scRipt>
	Other Info	
URL		http://testphp.vulnweb.com/search.php?test=query
	Method	POST
	Attack	<scrIpt>alert(1);</scRipt>
	Evidence	<scrIpt>alert(1);</scRipt>
	Other Info	
URL		http://testphp.vulnweb.com/secured/newuser.php
	Method	POST
	Attack	<scrIpt>alert(1);</scRipt>
	Evidence	<scrIpt>alert(1);</scRipt>
	Other Info	
URL		http://testphp.vulnweb.com/secured/newuser.php
	Method	POST
	Attack	<scrIpt>alert(1);</scRipt>
	Evidence	<scrIpt>alert(1);</scRipt>
	Other Info	
URL		http://testphp.vulnweb.com/secured/newuser.php
	Method	POST
	Attack	<scrIpt>alert(1);</scRipt>

	Evidence	<scrIpt>alert(1);</scRipt>
	Other Info	
URL		http://testphp.vulnweb.com/secured/newuser.php
	Method	POST
	Attack	<scrIpt>alert(1);</scRipt>
	Evidence	<scrIpt>alert(1);</scRipt>
	Other Info	
URL		http://testphp.vulnweb.com/secured/newuser.php
	Method	POST
	Attack	<scrIpt>alert(1);</scRipt>
	Evidence	<scrIpt>alert(1);</scRipt>
	Other Info	
URL		http://testphp.vulnweb.com/secured/newuser.php
	Method	POST
	Attack	<scrIpt>alert(1);</scRipt>
	Evidence	<scrIpt>alert(1);</scRipt>
	Other Info	
URL		http://testphp.vulnweb.com/userinfo.php
	Method	POST
	Attack	'"<scrIpt>alert(1);</scRipt>
	Evidence	'"<scrIpt>alert(1);</scRipt>
	Other Info	
URL		http://testphp.vulnweb.com/userinfo.php
	Method	POST
	Attack	'"<scrIpt>alert(1);</scRipt>
	Evidence	'"<scrIpt>alert(1);</scRipt>
	Other Info	
Instances		20
		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.

Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding module, and Apache Wicket.

Phases: Implementation; Architecture and Design

Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different |

	components, or when generating outputs that can contain multiple encodings at the same time, such as web pages or multi-part mail messages. Study all expected communication protocols and data representations to determine the required encoding strategies.
	For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanumeric characters.
	Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed.
	Phase: Architecture and Design
	For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can bypass the client-side checks by modifying values after the checks have been performed, or by changing the client to remove the client-side checks entirely. Then, these modified values would be submitted to the server.
Solution	If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.
	Phase: Implementation
	For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may choose a different encoding by guessing which encoding is actually being used by the web page. This can cause the web browser to treat certain sequences as special, opening up the client to subtle XSS attacks. See CWE-116 for more mitigations related to encoding/escaping.
	To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more recent versions of Internet Explorer and Firefox), this attribute can prevent the user's session cookie from being accessible to malicious client-side scripts that use document.cookie. This is not a complete solution, since HttpOnly is not supported by all browsers. More importantly, XMLHTTPRequest and other powerful browser technologies provide read access to HTTP headers, including the Set-Cookie header in which the HttpOnly flag is set.
	Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use an allow list of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a deny list). However, deny lists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright.
	When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue."
	Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or moved elsewhere.
Reference	https://owasp.org/www-community/attacks/xss/ https://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
Plugin Id	40012

High	**SQL Injection - MySQL**
Description	SQL injection may be possible.
URL	http://testphp.vulnweb.com/AJAX/infoartist.php?id=%27

	Method	GET
	Attack	'
	Evidence	You have an error in your SQL syntax
	Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL		http://testphp.vulnweb.com/AJAX/infocateg.php?id=%27
	Method	GET
	Attack	'
	Evidence	You have an error in your SQL syntax
	Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL		http://testphp.vulnweb.com/artists.php?artist=%27
	Method	GET
	Attack	'
	Evidence	You have an error in your SQL syntax
	Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL		http://testphp.vulnweb.com/listproducts.php?artist=%27
	Method	GET
	Attack	'
	Evidence	You have an error in your SQL syntax
	Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL		http://testphp.vulnweb.com/listproducts.php?cat=%27
	Method	GET
	Attack	'
	Evidence	You have an error in your SQL syntax
	Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL		http://testphp.vulnweb.com/product.php?pic=%27
	Method	GET
	Attack	'
	Evidence	You have an error in your SQL syntax
	Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.
URL		http://testphp.vulnweb.com/search.php?test=%27

Method	GET	
Attack	'	
Evidence	You have an error in your SQL syntax	
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.	
URL	http://testphp.vulnweb.com/AJAX/infotitle.php	
Method	POST	
Attack	'	
Evidence	You have an error in your SQL syntax	
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.	
URL	http://testphp.vulnweb.com/search.php?test=%27	
Method	POST	
Attack	'	
Evidence	You have an error in your SQL syntax	
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.	
URL	http://testphp.vulnweb.com/search.php?test=query	
Method	POST	
Attack	ZAP'	
Evidence	You have an error in your SQL syntax	
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.	
URL	http://testphp.vulnweb.com/secured/newuser.php	
Method	POST	
Attack	'	
Evidence	You have an error in your SQL syntax	
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.	
URL	http://testphp.vulnweb.com/userinfo.php	
Method	POST	
Attack	'	
Evidence	You have an error in your SQL syntax	
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.	
URL	http://testphp.vulnweb.com/userinfo.php	
Method	POST	

Attack	'	
Evidence	You have an error in your SQL syntax	
Other Info	RDBMS [MySQL] likely, given error message regular expression [\QYou have an error in your SQL syntax\E] matched by the HTML results. The vulnerability was detected by manipulating the parameter to cause a database error message to be returned and recognised.	
URL	http://testphp.vulnweb.com/AJAX/infotitle.php	
Method	POST	
Attack	1 and 0 in (select sleep(15)) --	
Evidence		
Other Info	The query time is controllable using parameter value [1 and 0 in (select sleep(15)) --], which caused the request to take [15,438] milliseconds, when the original unmodified query with value [1] took [0] milliseconds.	
URL	http://testphp.vulnweb.com/secured/newuser.php	
Method	POST	
Attack	qVPwBNsL' / sleep(15) / '	
Evidence		
Other Info	The query time is controllable using parameter value [qVPwBNsL' / sleep(15) / '], which caused the request to take [15,407] milliseconds, when the original unmodified query with value [qVPwBNsL] took [0] milliseconds.	
URL	http://testphp.vulnweb.com/userinfo.php	
Method	POST	
Attack	FbOMjHMM' / sleep(15) / '	
Evidence		
Other Info	The query time is controllable using parameter value [FbOMjHMM' / sleep(15) / '], which caused the request to take [15,414] milliseconds, when the original unmodified query with value [FbOMjHMM] took [0] milliseconds.	
Instances	16	
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply an 'allow list' of allowed characters, or a 'deny list' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact.	

	Grant the minimum database access that is necessary for the application.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html
CWE Id	89
WASC Id	19
Plugin Id	40018

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

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

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

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

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

	Method	GET
	Attack	
	Evidence	`<form name='f_addcart' method='POST' action='cart.php'>`
	Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "addcart" "price"].
URL		http://testphp.vulnweb.com/product.php?pic=4
	Method	GET
	Attack	
	Evidence	`<form action="search.php?test=query" method="post">`
	Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL		http://testphp.vulnweb.com/product.php?pic=5
	Method	GET
	Attack	
	Evidence	`<form name='f_addcart' method='POST' action='cart.php'>`
	Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "addcart" "price"].
URL		http://testphp.vulnweb.com/product.php?pic=5
	Method	GET
	Attack	
	Evidence	`<form action="search.php?test=query" method="post">`
	Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL		http://testphp.vulnweb.com/product.php?pic=6
	Method	GET
	Attack	
	Evidence	`<form name='f_addcart' method='POST' action='cart.php'>`
	Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "addcart" "price"].
URL		http://testphp.vulnweb.com/product.php?pic=6
	Method	GET
	Attack	
	Evidence	`<form action="search.php?test=query" method="post">`
	Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL		http://testphp.vulnweb.com/product.php?pic=7
	Method	GET

	Attack	
	Evidence	<form name='f_addcart' method='POST' action='cart.php'>
	Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "addcart" "price"].
URL		http://testphp.vulnweb.com/product.php?pic=7
	Method	GET
	Attack	
	Evidence	<form action="search.php?test=query" method="post">
	Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL		http://testphp.vulnweb.com/search.php?test=query
	Method	GET
	Attack	
	Evidence	<form action="search.php?test=query" method="post">
	Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
URL		http://testphp.vulnweb.com/signup.php
	Method	GET
	Attack	
	Evidence	<form name="form1" method="post" action="/secured/newuser.php">
	Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "signup" "ucc" "uemail" "upass" "upass2" "uphone" "urname" "uuname"].
URL		http://testphp.vulnweb.com/signup.php
	Method	GET
	Attack	
	Evidence	<form action="search.php?test=query" method="post">
	Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 2: "goButton" "searchFor"].
URL		http://testphp.vulnweb.com/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, _csrfToken] 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, _csrfToken] 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, _csrfToken] 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, _csrfToken] was found in the following HTML form: [Form 1: "goButton" "searchFor"].
Instances		42
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	Application Error Disclosure
Description	This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
URL	http://testphp.vulnweb.com/AJAX/infotitle.php
Method	GET
Attack	
Evidence	You have an error in your SQL syntax
Other Info	
Instances	1
Solution	Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
Reference	
CWE Id	550
WASC Id	13
Plugin Id	90022

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
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/
Method	GET
Attack	
Evidence	
Other Info	

	URL	http://testphp.vulnweb.com/AJAX/
	Method	GET
	Attack	
	Evidence	
	Other Info	
	URL	http://testphp.vulnweb.com/AJAX/index.php
	Method	GET
	Attack	
	Evidence	
	Other Info	
	URL	http://testphp.vulnweb.com/AJAX/showxml.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/Flash/
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/images/
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-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-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/BuyProduct-3/	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details	
Method	GET	

Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
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/color-printer/3/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
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/network-attached-storage-dlink/1/
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
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/Details/web-camera-a4tech/2/	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/	
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/search.php?test=query	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/secured/	
Method	GET	
Attack		
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/secured/newuser.php	
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	71
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	Directory Browsing
Description	It is possible to view a listing of the directory contents. Directory listings may reveal hidden scripts, include files, backup source files, etc., which can be accessed to reveal sensitive information.
URL	http://testphp.vulnweb.com/Flash/
Method	GET
Attack	
Evidence	<title>Index of /Flash/</title>
Other Info	Web server identified: Apache 2
URL	http://testphp.vulnweb.com/images/

Method	GET	
Attack		
Evidence	<title>Index of /images/</title>	
Other Info	Web server identified: Apache 2	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/	
Method	GET	
Attack		
Evidence	<title>Index of /Mod_Rewrite_Shop/images/</title>	
Other Info	Web server identified: Apache 2	
Instances	3	
Solution	Configure the web server to disable directory browsing.	
Reference	https://cwe.mitre.org/data/definitions/548.html	
CWE Id	548	
WASC Id	16	
Plugin Id	10033	

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

URL	http://testphp.vulnweb.com/AJAX/showxml.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/Flash/	
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/images/	
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/images/	
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/search.php?test=query
Method	GET
Attack	
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured/newuser.php
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	53	
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	

Medium	XSLT Injection

Description	Injection using XSL transformations may be possible, and may allow an attacker to read system information, read and write files, or execute arbitrary code.
URL	http://testphp.vulnweb.com/showimage.php?file=%3Cxsl%3Avalue-of+select%3D%22document%28%27http%3A%2F%2Ftestphp.vulnweb.com%3A22%27%29%22%2F%3E
Method	GET
Attack	<xsl:value-of select="document('http://testphp.vulnweb.com:22')"/>
Evidence	failed to open stream
Other Info	Port scanning may be possible.
Instances	1
Solution	Sanitize and analyze every user input coming from any client-side.
Reference	https://www.contextis.com/blog/xslt-server-side-injection-attacks
CWE Id	91
WASC Id	23
Plugin Id	90017

Low	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	http://testphp.vulnweb.com
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/
Method	GET
Attack	
Evidence	X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Other Info	
URL	http://testphp.vulnweb.com/AJAX/
Method	GET
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/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/infocateg.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/infocateg.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/infocateg.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/infocateg.php?id=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/AJAX/infotitle.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	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/search.php?test=query
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/secured/
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/secured/newuser.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/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/infotitle.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/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	84

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

Low	Server Leaks Version Information via "Server" HTTP Response Header Field
Description	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	http://testphp.vulnweb.com
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
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/infocateg.php?id=1	
Method	GET	
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=2	
Method	GET	
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=3	
Method	GET	
Attack		
Evidence	nginx/1.19.0	

Other Info	
URL	http://testphp.vulnweb.com/AJAX/infocateg.php?id=4
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/infotitle.php
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/AJAX/showxml.php
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
	Method	GET
	Attack	
	Evidence	nginx/1.19.0
	Other Info	
URL		http://testphp.vulnweb.com/Flash/
	Method	GET
	Attack	
	Evidence	nginx/1.19.0
	Other Info	
URL		http://testphp.vulnweb.com/Flash/add.fla
	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/	
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	
Method	GET	
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/images/	
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/	
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-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-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/BuyProduct-3/
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
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/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
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/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
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/Details/web-camera-a4tech/2/
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Method	GET
Attack	
Evidence	nginx/1.19.0
Other Info	

URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images/	
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/search.php?test=query	
Method	GET	
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/secured	
Method	GET	
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/secured/	
Method	GET	
Attack		
Evidence	nginx/1.19.0	
Other Info		
URL	http://testphp.vulnweb.com/secured/newuser.php	
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/infotitle.php	
Method	POST	
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	118	
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.	
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/	
CWE Id	497	
WASC Id	13	
Plugin Id	10036	

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

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	http://testphp.vulnweb.com/AJAX/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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/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/infocateg.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/infocateg.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/infocateg.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/infocateg.php?id=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/AJAX/infotitle.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/showxml.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/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/	
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.fla	
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		
	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/images/	
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	This issue still applies to error type pages (401, 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/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/
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		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.	
URL	http://testphp.vulnweb.com/search.php?test=query	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.	
URL	http://testphp.vulnweb.com/secured/newuser.php	
Method	GET	
Attack		
Evidence		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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		
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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/infotitle.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/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	91	
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=fFOtSgdq passwordParam=upass referer=http://testphp.vulnweb.com/signup.php
URL	http://testphp.vulnweb.com/secured/newuser.php
Method	POST
Attack	
Evidence	upass
Other Info	userParam=uemail userValue=qYbVruxo passwordParam=upass referer=http://testphp.vulnweb.com/signup.php
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	3
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
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
URL	http://testphp.vulnweb.com/

Method	GET	
Attack		
Evidence		
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.	
URL	http://testphp.vulnweb.com/AJAX/	
Method	GET	
Attack		
Evidence		
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-1] do not match.	
URL	http://testphp.vulnweb.com/AJAX/index.php	
Method	GET	
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 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
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/search.php?test=query	
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/secured/newuser.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/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	35	
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.	
Reference	https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection	
CWE Id	436	
WASC Id	15	
Plugin Id	90011	

Informational	GET for POST
Description	A request that was originally observed as a POST was also accepted as a GET. This issue does not represent a security weakness unto itself, however, it may facilitate simplification of other attacks. For example if the original POST is subject to Cross-Site Scripting (XSS), then this finding may indicate that a simplified (GET based) XSS may also be possible.
URL	http://testphp.vulnweb.com/cart.php
Method	GET
Attack	
Evidence	GET http://testphp.vulnweb.com/cart.php?addcart=7&price=15000 HTTP/1.1

Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Attack	
Evidence	GET http://testphp.vulnweb.com/guestbook.php?name=ZAP&submit=add%20message&text= HTTP/1.1
Other Info	
URL	http://testphp.vulnweb.com/search.php?test=query
Method	GET
Attack	
Evidence	GET http://testphp.vulnweb.com/search.php?goButton=go&searchFor=ZAP HTTP/1.1
Other Info	
Instances	3
Solution	Ensure that only POST is accepted where POST is expected.
Reference	
CWE Id	16
WASC Id	20
Plugin Id	10058

Informational	Modern Web Application
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://testphp.vulnweb.com/AJAX/
Method	GET
Attack	
Evidence	titles
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	http://testphp.vulnweb.com/AJAX/index.php
Method	GET
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	`<a href='#' onClick="window.open('./comment.php?aid=1','comment','width=500,height=400')">comment on this artist</a>`
	Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL		http://testphp.vulnweb.com/artists.php?artist=2
	Method	GET
	Attack	
	Evidence	`<a href='#' onClick="window.open('./comment.php?aid=2','comment','width=500,height=400')">comment on this artist</a>`
	Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL		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	10
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	User Agent Fuzzer
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	http://testphp.vulnweb.com/AJAX
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/AJAX
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/AJAX
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/AJAX
	Method	GET
	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/AJAX
	Method	GET
	Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/AJAX
	Method	GET
	Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/AJAX
	Method	GET
	Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Flash
	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Flash
	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Flash
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	

Other Info		
URL	http://testphp.vulnweb.com/Flash	
Method	GET	
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Flash	
Method	GET	
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Flash	
Method	GET	
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/guestbook.php	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/guestbook.php	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/guestbook.php	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/guestbook.php	
Method	GET	
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko	
Evidence		

	Other Info	
	URL	http://testphp.vulnweb.com/guestbook.php
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
	Evidence	
	Other Info	
	URL	http://testphp.vulnweb.com/guestbook.php
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
	Evidence	
	Other Info	
	URL	http://testphp.vulnweb.com/guestbook.php
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
	Evidence	
	Other Info	
	URL	http://testphp.vulnweb.com/guestbook.php
	Method	GET
	Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
	Evidence	
	Other Info	
	URL	http://testphp.vulnweb.com/guestbook.php
	Method	GET
	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
	Evidence	
	Other Info	
	URL	http://testphp.vulnweb.com/guestbook.php
	Method	GET
	Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
	Evidence	
	Other Info	
	URL	http://testphp.vulnweb.com/guestbook.php
	Method	GET
	Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
	Evidence	

Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/high
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/high
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/hpp
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other	

	Info	
	URL	http://testphp.vulnweb.com/hpp
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
	Evidence	
	Other Info	
	URL	http://testphp.vulnweb.com/hpp
	Method	GET
	Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
	Evidence	
	Other Info	
	URL	http://testphp.vulnweb.com/hpp
	Method	GET
	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
	Evidence	
	Other Info	
	URL	http://testphp.vulnweb.com/hpp
	Method	GET
	Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
	Evidence	
	Other Info	
	URL	http://testphp.vulnweb.com/hpp
	Method	GET
	Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
	Evidence	
	Other Info	
	URL	http://testphp.vulnweb.com/hpp
	Method	GET
	Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
	Evidence	
	Other Info	
	URL	http://testphp.vulnweb.com/images
	Method	GET
	Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
	Evidence	
	Other Info	

URL	http://testphp.vulnweb.com/images	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/images	
Method	GET	
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/images	
Method	GET	
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/images	
Method	GET	
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/images	
Method	GET	
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/images	
Method	GET	
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/images	
Method	GET	
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)	
Evidence		
Other Info		

URL	http://testphp.vulnweb.com/images		
Method	GET		
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4		
Evidence			
Other Info			
URL	http://testphp.vulnweb.com/images		
Method	GET		
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16		
Evidence			
Other Info			
URL	http://testphp.vulnweb.com/images		
Method	GET		
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)		
Evidence			
Other Info			
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop		
Method	GET		
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)		
Evidence			
Other Info			
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop		
Method	GET		
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)		
Evidence			
Other Info			
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop		
Method	GET		
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)		
Evidence			
Other Info			
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop		
Method	GET		
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko		
Evidence			
Other Info			
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop		

Method	GET	
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop	
Method	GET	
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop	
Method	GET	
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop	
Method	GET	
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop	
Method	GET	
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop	
Method	GET	
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop	
Method	GET	
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1	

	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
	Method	GET
	Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
	Method	GET
	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
	Method	GET
	Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
	Method	GET
	Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1
	Method	GET
	Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
	Method	GET

Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET

Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko

	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
	Method	GET
	Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
	Method	GET
	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
	Method	GET
	Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
	Method	GET
	Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details
	Method	GET
	Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	

	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
	Method	GET
	Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
	Method	GET
	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
	Method	GET
	Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
	Method	GET
	Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3
	Method	GET
	Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
	Evidence	

Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other	

	Info
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	

URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/web-camera-a4tech/2
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images

Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images	
Method	GET	
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images	
Method	GET	
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images	
Method	GET	
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images	
Method	GET	
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images	
Method	GET	
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/Mod_Rewrite_Shop/images	

	Method	GET
	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
	Method	GET
	Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
	Method	GET
	Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/Mod_Rewrite_Shop/images
	Method	GET
	Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/robots.txt
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/robots.txt
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/robots.txt
	Method	GET
	Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/robots.txt
	Method	GET

Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/robots.txt	
Method	GET	
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/robots.txt	
Method	GET	
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/robots.txt	
Method	GET	
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/secured	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/secured	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/secured	
Method	GET	
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/secured	
Method	GET	

Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Method	GET

Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/secured
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18

Attack	(KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/sitemap.xml
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/userinfo.php
	Method	GET
	Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/userinfo.php
	Method	GET
	Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/userinfo.php
	Method	GET
	Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/userinfo.php
	Method	GET
	Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/userinfo.php
	Method	GET
	Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/userinfo.php
	Method	GET
	Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
	Evidence	
	Other Info	
URL		http://testphp.vulnweb.com/guestbook.php
	Method	POST
	Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	

Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/guestbook.php
Method	POST
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://testphp.vulnweb.com/userinfo.php
Method	POST
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	

Other Info		
URL	http://testphp.vulnweb.com/userinfo.php	
Method	POST	
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/userinfo.php	
Method	POST	
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/userinfo.php	
Method	POST	
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/userinfo.php	
Method	POST	
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/userinfo.php	
Method	POST	
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/userinfo.php	
Method	POST	
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16	
Evidence		
Other Info		
URL	http://testphp.vulnweb.com/userinfo.php	
Method	POST	
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)	
Evidence		

Other Info	
Instances	218
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

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](#)