

ZAP_{by} Checkmar× ZAP by Checkmarx Scanning Report

Site: http://testphp.vulnweb.com

Generated on Sat, 8 Mar 2025 12:14:06

ZAP Version: 2.16.0

ZAP by Checkmarx

Summary of Alerts

| Risk Level | Number of Alerts |
|---------------|------------------|
| High | 0 |
| Medium | 3 |
| Low | 3 |
| Informational | 4 |

Alerts

| Name | Risk Level | Number of Instances |
|---|---------------|------------------------|
| Absence of Anti-CSRF Tokens | Medium | 40 |
| Content Security Policy (CSP) Header Not Set | Medium | 52 |
| Missing Anti-clickjacking Header | Medium | 45 |
| Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) | Low | 77 |
| Server Leaks Version Information via "Server" HTTP Response Header Field | Low | 90 |
| X-Content-Type-Options Header Missing | Low | 81 |
| Authentication Request Identified | Informational | 2 |
| <u>Charset Mismatch (Header Versus Meta Content-Type Charset)</u> | Informational | 31 |
| Modern Web Application | Informational | 9 |
| <u>User Controllable HTML Element Attribute</u> (<u>Potential XSS</u>) | Informational | 4 |

Alert Detail

| Medium | Absence of Anti-CSRF Tokens |
|--------|---|
| | No Anti-CSRF tokens were found in a HTML submission form. |
| | A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL |

| Description | /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. 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
|---------------|--|
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> | |
|--|--|
| No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, | |
| Other csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_to Infocsrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the follo 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"></form> | |
| No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_to Info | |
| URL http://testphp.vulnweb.com/login.php | |
| Method GET | |
| Attack | |
| Evidence <form action="userinfo.php" method="post" name="loginform"></form> | |
| No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_to _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the follo 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"></form> | |
| No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, Csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_to Info | |
| URL http://testphp.vulnweb.com/product.php?pic=1 | |
| Method GET | |
| Attack | |
| Evidence <form action="cart.php" method="POST" name="f_addcart"></form> | |
| No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_to Info | |
| URL http://testphp.vulnweb.com/product.php?pic=1 | |
| Method GET | |
| Attack | |
| Evidence <form action="search.php?test=query" method="post"></form> | |
| No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_to lnfo | |
| URL http://testphp.vulnweb.com/product.php?pic=2 | |
| Method GET | |
| Attack | |
| | |

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

| Oil | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, |
|---------------|--|
| Other Info | csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "addcart" "price"]. |
| URL | http://testphp.vulnweb.com/product.php?pic=5 |
| Method | GET |
| Attack | |
| Evidence | <form action="search.php?test=query" method="post"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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 action="cart.php" method="POST" name="f_addcart"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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 action="cart.php" method="POST" name="f_addcart"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 2: "goButton" "searchFor"]. |
| URL | http://testphp.vulnweb.com/signup.php |
| Method | GET |
| Attack | |
| Evidence | <form action="/secured/newuser.php" method="post" name="form1"></form> |
| | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, |

| Other Info | csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] 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"></form> |
| Other Info | No known Anti-CSRF token [anticsrf, CSRFToken,RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret,csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "goButton" "searchFor"]. |
| Instances | 40 |
| | 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). |
| Solution | Note that this can be bypassed using XSS. |
| | Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. |
| | Note that this can be bypassed using XSS. |
| | Use the ESAPI Session Management control. |
| | This control includes a component for CSRF. |
| | Do not use the GET method for any request that triggers a state change. |
| | Phase: Implementation |
| | Check the HTTP Referer header to see if the request originated from an expected page. |
| | This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons. |
| Reference | https://cheatsheetseries.owasp.org/cheatsheets/Cross- Site Request Forgery Prevention Cheat Sheet.html https://cwe.mitre.org/data/definitions/352.html |
| CWE Id | <u>352</u> |
| WASC Id | 9 |
| Plugin Id | 10202 |
| Medium | Content Security Policy (CSP) Header Not Set |
| Description | Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files. |
| URL | http://testphp.vulnweb.com/ |
| 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/artists.php |
|---------------|---|
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/artists.php?artist=1 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/artists.php?artist=2 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/artists.php?artist=3 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/cart.php |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/categories.php |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/comment.php?aid=1 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/comment.php?aid=2 |
| Method | GET |

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

| 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 | |
| | |

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

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

| 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 | 52 |
| Solution | Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header. |
| | 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 |
| Reference | https://www.w3.org/TR/CSP/ |
| | |

| | https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/ |
|-----------|--|
| CWE Id | <u>693</u> |
| WASC Id | 15 |
| Plugin Id | 10038 |

| Plugin Id | 10038 |
|---------------|---|
| Medium | Missing Anti-clickjacking Header |
| Description | The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options. |
| URL | http://testphp.vulnweb.com/ |
| 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/artists.php |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/artists.php?artist=1 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/artists.php?artist=2 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/artists.php?artist=3 |
| Method | GET |
| Attack | |
| Evidence | |

| Other Info | |
|---------------|---|
| URL | http://testphp.vulnweb.com/cart.php |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/categories.php |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/disclaimer.php |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/guestbook.php |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/hpp/ |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/hpp/?pp=12 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/hpp/params.php?p=valid&pp=12 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| | |

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

| Attack | |
|---|---|
| Evidence | |
| Other | |
| Info | |
| URL | http://testphp.vulnweb.com/login.php |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/Mod_Rewrite_Shop/ |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/ |
| Method | GET |
| Attack | |
| Evidence | |
| Other | |
| Info | |
| Info URL | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ |
| | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ GET |
| URL | |
| URL Method | |
| URL Method Attack | |
| URL Method Attack Evidence Other | |
| URL Method Attack Evidence Other Info | GET |
| URL Method Attack Evidence Other Info URL | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ |
| URL Method Attack Evidence Other Info URL Method | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ |
| URL Method Attack Evidence Other Info URL Method Attack | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ |
| URL Method Attack Evidence Other Info URL Method Attack Evidence Other | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ |
| URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET |
| URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL URL URL URL URL URL URL UR | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/ |
| URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Method Attack Evidence Other Info URL Method | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/ |
| URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/ |
| URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Other Info | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/ |
| URL Method Attack Evidence Other Info | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/. GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/. GET |
| URL Method Attack Evidence Other Info URL | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/ GET http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/ |

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

| Info | |
|---------------|--|
| URL | http://testphp.vulnweb.com/product.php?pic=4 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=5 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=6 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=7 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/signup.php |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/AJAX/showxml.php |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/cart.php |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/guestbook.php |

| Method | POST |
|---------------|--|
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/search.php?test=query |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | http://testphp.vulnweb.com/secured/newuser.php |
| Method | POST |
| Attack | |
| Evidence | |
| Other | |
| Info | 45 |
| Instances | Modern Web browsers support the Content Security Policy and V Frame Ontions LITTE |
| | 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. |
| Solution | If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive. |
| Reference | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options |
| CWE Id | 1021 |
| WASC Id | 15 |
| Plugin Id | 10020 |
| Low | Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) |
| Description | The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to. |
| URL | http://testphp.vulnweb.com/ |
| 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 |

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

| 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 | |
| LIDI | http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-1.html |
| URL | http://testprip.vuinweb.com/woo_Kewnite_Shop/KateProduct-1.html |
| Method | GET |
| | |
| Method | |
| Method Attack | GET |
| Method Attack Evidence Other | GET |
| Method Attack Evidence Other Info | GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 |
| Method Attack Evidence Other Info URL | X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html |
| Method Attack Evidence Other Info URL Method | X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html |
| Method Attack Evidence Other Info URL Method Attack | GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html GET |
| Method Attack Evidence Other Info URL Method Attack Evidence Other | GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html GET |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info | X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL URL URL URL URL URL URL | X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method | X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Attack Attack | X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html GET |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other | X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html GET |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Other Info | GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL Method Attack Evidence Other Info URL Method | GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/privacy.php |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL Method Attack Evidence URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info | GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html GET X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 http://testphp.vulnweb.com/privacy.php |

| Other Info | |
|---------------|--|
| URL | http://testphp.vulnweb.com/product.php?pic=1 |
| Method | GET |
| Attack | |
| Evidence | X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=2 |
| Method | GET |
| Attack | |
| Evidence | X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=3 |
| Method | GET |
| Attack | |
| Evidence | X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=4 |
| Method | GET |
| Attack | |
| Evidence | X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=5 |
| Method | GET |
| Attack | |
| Evidence | X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=6 |
| Method | GET |
| Attack | |
| Evidence | X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=7 |
| Method | GET |
| Attack | |
| Evidence | X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1 |
| Other Info | |

| URL | http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild. |
|---------------|---|
| | nodeValue%20+%20' GET |
| Method | GET |
| Attack | V. Davidson d. Div. DI ID/5 0. 40. 00 v. hv. intv 00. 04. 4 v. delt. avenu area 4 |
| 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 | http://teataba.vulayyab.com/accured/ac |
| 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 | 77 |
| 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 |
| Low Description | Server Leaks Version Information via "Server" HTTP Response Header Field 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. |
| | The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities |
| 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. |
| Description URL | 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. http://testphp.vulnweb.com/ |
| Description URL Method | 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. http://testphp.vulnweb.com/ |
| Description URL Method Attack | 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. http://testphp.vulnweb.com/ GET |
| Description URL Method Attack Evidence Other | 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. http://testphp.vulnweb.com/ GET |
| Description URL Method Attack Evidence Other Info | 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. http://testphp.vulnweb.com/ GET nginx/1.19.0 |
| Description URL Method Attack Evidence Other Info URL | 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. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/artists.php |
| Description URL Method Attack Evidence Other Info URL Method | 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. http://testphp.vulnweb.com/ GET nginx/1.19.0 http://testphp.vulnweb.com/AJAX/artists.php GET |
| Description URL Method Attack Evidence Other Info URL Method Attack | 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. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/artists.php |
| Description URL Method Attack Evidence Other Info URL Method Attack Evidence Other | 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. http://testphp.vulnweb.com/ GET nginx/1.19.0 http://testphp.vulnweb.com/AJAX/artists.php GET |
| Description URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info | 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. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/artists.php GET nginx/1.19.0 |
| Description URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL URL Method Attack URL URL URL URL URL URL URL UR | 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. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/artists.php GET nginx/1.19.0 http://testphp.vulnweb.com/AJAX/categories.php |
| Description URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL Method Method Method URL Method | 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. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/artists.php GET nginx/1.19.0 http://testphp.vulnweb.com/AJAX/categories.php |
| Description URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack | 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. http://testphp.vulnweb.com/ GET http://testphp.vulnweb.com/AJAX/artists.php GET nginx/1.19.0 http://testphp.vulnweb.com/AJAX/categories.php GET |

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

| Evidence | nginx/1.19.0 |
|---------------|--|
| Other Info | |
| URL | http://testphp.vulnweb.com/categories.php |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/comment.php?aid=1 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/comment.php?aid=2 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/comment.php?aid=3 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/disclaimer.php |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/favicon.ico |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/Flash/add.swf |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other | |

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

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

| Attack | |
|---|--|
| Evidence | nginx/1.19.0 |
| Other | |
| Info | |
| URL | http://testphp.vulnweb.com/login.php |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/Mod_Rewrite_Shop/ |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/ |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| | |
| URL | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ |
| URL Method | http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ GET |
| | GET |
| Method | |
| Method Attack | GET |
| Method Attack Evidence Other | GET |
| Method Attack Evidence Other Info | GET nginx/1.19.0 |
| Method Attack Evidence Other Info URL | nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ |
| Method Attack Evidence Other Info URL Method | nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ |
| Method Attack Evidence Other Info URL Method Attack | nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET |
| Method Attack Evidence Other Info URL Method Attack Evidence Other | nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info | nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET nginx/1.19.0 |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL URL URL URL URL URL URL URL | nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/ |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method | nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/ |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Attack Attack Attack Attack Attack | nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/ GET |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other | nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/ GET |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Other Info | nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/ GET nginx/1.19.0 |
| Method Attack Evidence Other Info URL Method Attack URL Method Attack URL URL URL URL URL URL URL | nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/ GET nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/ |
| Method Attack Evidence Other Info URL Method Attack Evidence Other Info | nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ GET nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/color-printer/3/ GET nginx/1.19.0 http://testphp.vulnweb.com/Mod_Rewrite_Shop/Details/network-attached-storage-dlink/1/ |

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

| URL | http://testphp.vulnweb.com/privacy.php |
|---------------|--|
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other | |
| Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=1 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=2 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=3 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=4 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=5 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=6 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/product.php?pic=7 |
| Method | GET |
| | |

| Attack | |
|---------------|---|
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/robots.txt |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/secured/style.css |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/showimage.php?file='%20+%20pict.item(0).firstChild.nodeValue%20+%20' |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/showimage.php?file=./pictures/1.jpg&size=160 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/showimage.php?file=./pictures/2.jpg&size=160 |
| Method | GET |
| Attack | |
| | |

| Evidence | nginx/1.19.0 |
|---------------|---|
| Other Info | |
| URL | http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/showimage.php?file=./pictures/3.jpg&size=160 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/showimage.php?file=./pictures/4.jpg&size=160 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/showimage.php?file=./pictures/5.jpg&size=160 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other | |

| Info | |
|---------------|---|
| URL | http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg&size=160 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/showimage.php?file=./pictures/7.jpg&size=160 |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/signup.php |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/sitemap.xml |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/style.css |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/userinfo.php |
| Method | GET |
| Attack | |
| Evidence | nginx/1.19.0 |
| Other Info | |
| URL | http://testphp.vulnweb.com/AJAX/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 | 90 |
| 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 |
| | 1444 |
| 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/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/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 | |
| | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still |
| | |

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

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

| Other Info advay from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still other affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected to the responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ Method GET | | |
|--|---|--|
| Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/. Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by inje | URL | http://testphp.vulnweb.com/listproducts.php?cat=4 |
| Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/login.php Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/ Other affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for b | Method | GET |
| This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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/Buy/Product-1/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still one away from 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/Buy/Product-1/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still one away from their actual content type. At "High" threshold his scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/Buy/Product-2/ Method GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still one or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/Buy/Product-2/ Method GET This issue still applies to error t | Attack | |
| Other Info affected by injection issues, in which case there is still concern for browsers sniffing pages when the case trace or server error responses. URL http://testphp.vulnweb.com/login.php Method GET Other Info affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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/ 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/Mod_Rewrite_Shop/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still one or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still one or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still of affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still other or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ Method GET Attack Evidence This issue still applies to error type pages (401, | Evidence | |
| Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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/ This issue still appli | | away from their actual content type. At "High" threshold this scan rule will not alert on client |
| Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/ Method GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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/ GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages which away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages to server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages to server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ Method GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages. This issue still applies to error type pages (401, 403, 50 | URL | http://testphp.vulnweb.com/login.php |
| This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/. Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 | Method | GET |
| Other Info | Attack | |
| Other Info adjected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still other 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of server error for browsers sniffing pages are forten still affected by injection issues, in which case there is still concern for browsers sniffing pages are forten still affected by injection issues, in whi | Evidence | |
| Method Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still other affected by injection issues, in which case there is still concern for browsers sniffing pages are often still other affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the away from their actual content type. At "High" threshold this scan rule will not alert on client of the away from their actual content type. At "High" threshold this scan rule will not alert on client of the away from the | | away from their actual content type. At "High" threshold this scan rule will not alert on client |
| Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still and the 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern fo | URL | http://testphp.vulnweb.com/Mod_Rewrite_Shop/ |
| Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-1/ GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of server type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the affected by injection issues, in which case | Method | GET |
| Other Info | Attack | |
| 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/Mod_Rewrite_Shop/BuyProduct-1/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case there is still concern for browsers sniffing pages affected by injection issues, in which case t | Evidence | |
| Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client | | away from their actual content type. At "High" threshold this scan rule will not alert on client |
| Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/Mod Rewrite Shop/BuyProduct-2/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client | LIRI | http://teetabp.yullpweb.com/Med. Bourite. Shop/Buy/Bradust 1/ |
| Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still other affected by injection issues, in which case there is still concern for browsers sniffing pages are often still other affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client of the pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers and the page are often still | OILL | http://testphp.vuinweb.com/wiod_Rewrite_Shop/BuyProduct-1/ |
| This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client | | |
| Other Info adjected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still other affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client other away from their actual content type. At "High" threshold this scan rule will not alert on client of the recommendation of the scan rule will not alert on client affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client | Method | |
| Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client | Method Attack | |
| Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client | Method 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 away from their actual content type. At "High" threshold this scan rule will not alert on client |
| Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. URL http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client | Method Attack Evidence Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. |
| Other Info Other Info Other Info Other Info Other Info Info Info Info Info Info Info Info | Method Attack Evidence Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ |
| Other Info adjected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client | Method Attack Evidence Other Info URL Method | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ |
| Method GET Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages lnfo away from their actual content type. At "High" threshold this scan rule will not alert on client | Method Attack Evidence Other Info URL Method Attack | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ |
| Attack Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages lnfo away from their actual content type. At "High" threshold this scan rule will not alert on client | Method Attack Evidence Other Info URL Method 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 away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client |
| Evidence This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client | Method Attack Evidence Other Info URL Method Attack Evidence Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. |
| This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still other affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client | Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL URL URL URL URL URL URL | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ |
| Other affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client | Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ |
| | Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Attack | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-2/ GET This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. http://testphp.vulnweb.com/Mod_Rewrite_Shop/BuyProduct-3/ |

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

| Method | GET |
|---------------|--|
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. |
| URL | http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-2.html |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. |
| URL | http://testphp.vulnweb.com/Mod_Rewrite_Shop/RateProduct-3.html |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. |
| URL | http://testphp.vulnweb.com/product.php?pic=1 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. |
| URL | http://testphp.vulnweb.com/product.php?pic=2 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. |
| URL | http://testphp.vulnweb.com/product.php?pic=3 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses. |
| URL | http://testphp.vulnweb.com/product.php?pic=4 |
| | |

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

| Attack | |
|---------------|--|
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from 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 | 81 |
| | 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. |
| Solution | 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 |
| | |

| 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=syrqVnMU 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 | 2 |
| 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 | <u>10111</u> |
| 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/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 | There was a charset mismatch between the HTTP Header and the META content-type |
| Info | encoding declarations: [UTF-8] and [iso-8859-2] do not match. |
| URL | encoding declarations: [UTF-8] and [iso-8859-2] do not match. http://testphp.vulnweb.com/artists.php?artist=1 |

Attack

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

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

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

| Attack | |
|---------------|--|
| Evidence | |
| Other Info | There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match. |
| URL | http://testphp.vulnweb.com/signup.php |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match. |
| URL | http://testphp.vulnweb.com/cart.php |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match. |
| URL | http://testphp.vulnweb.com/guestbook.php |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match. |
| URL | http://testphp.vulnweb.com/search.php?test=query |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match. |
| URL | http://testphp.vulnweb.com/secured/newuser.php |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-1] do not match. |
| Instances | 31 |
| Solution | Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML. |
| Reference | https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection |
| CWE Id | <u>436</u> |
| WASC Id | 15 |
| Plugin Id | 90011 |
| Informational | Modern Web Application |

| Informational | Modern Web Application |
|---------------|--|
| Description | The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one. |
| | |

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

| Other Info | Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application. |
|--|---|
| URL | http://testphp.vulnweb.com/listproducts.php?cat=1 |
| Method | GET |
| Attack | |
| Evidence | comment on this picture |
| Other Info | Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application. |
| URL | http://testphp.vulnweb.com/listproducts.php?cat=2 |
| Method | GET |
| Attack | |
| Evidence | comment on this picture |
| Other Info | Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application. |
| Instances | 9 |
| Solution | This is an informational alert and so no changes are required. |
| Reference | |
| CWE Id | |
| WASC Id | |
| Plugin Id | 10109 |
| Informational | Hear Controlled a UTML Flower Av. II. (/P. (. /L. 1900) |
| 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. |
| | 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 |
| 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. |
| Description URL | 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. http://testphp.vulnweb.com/guestbook.php |
| Description URL Method | 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. http://testphp.vulnweb.com/guestbook.php |
| Description URL Method Attack | 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. http://testphp.vulnweb.com/guestbook.php |
| Description URL Method Attack Evidence Other | 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. http://testphp.vulnweb.com/guestbook.php POST 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 |
| Description URL Method Attack Evidence Other Info | 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. http://testphp.vulnweb.com/guestbook.php POST 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 |
| Description URL Method Attack Evidence Other Info URL | 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. http://testphp.vulnweb.com/guestbook.php POST 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 http://testphp.vulnweb.com/guestbook.php |
| Description URL Method Attack Evidence Other Info URL Method | 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. http://testphp.vulnweb.com/guestbook.php POST 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 http://testphp.vulnweb.com/guestbook.php |
| Description URL Method Attack Evidence Other Info URL Method Attack | 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. http://testphp.vulnweb.com/guestbook.php POST 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 http://testphp.vulnweb.com/guestbook.php |
| Description URL Method Attack Evidence Other Info URL Method Attack Evidence Other | 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. http://testphp.vulnweb.com/guestbook.php POST 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 http://testphp.vulnweb.com/guestbook.php POST 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 |
| Description URL Method Attack Evidence Other Info URL Method Attack Evidence Other | 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. http://testphp.vulnweb.com/guestbook.php POST 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 http://testphp.vulnweb.com/guestbook.php POST 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 |
| Description URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack URL Method Attack URL URL URL URL URL | 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. http://testphp.vulnweb.com/guestbook.php POST 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 http://testphp.vulnweb.com/guestbook.php POST 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 http://testphp.vulnweb.com/search.php?test=query |
| Description URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method Attack Evidence Other Info URL Method | 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. http://testphp.vulnweb.com/guestbook.php POST 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 http://testphp.vulnweb.com/guestbook.php POST 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 http://testphp.vulnweb.com/search.php?test=query |

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