VulnScan Report - 2024-11-28 13:54:23

Target Domain: ecampus.psgtech.ac.in
IP Address: 103.224.33.45
Scan Options: []

Vulnerability Information:

```
Spider and Ajax Spider scanning http://ecampus.psgtech.ac.in initiated.
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
```

```
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
'Records to passive scan : ' + zap.pscan.records_to_scan
Passive Scan completed
Hosts: ecampus.psgtech.ac.in, ecampus.psgtech.ac.in
Alerts:
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1', 'inputVector':
'', 'url': 'http://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '0', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1', 'inputVector': '', 'url':
'http://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.or
```

g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '1', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '3', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header', 'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id': '2', 'alertRef': '10020-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525', 'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.', 'messageId': '3', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-recommendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control', 'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '3', 'alertRef': '10015'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '3', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt

ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '4', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '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: "__VIEWSTATE" "__VIEWSTATEGENERATOR"].', 'method': 'GET', 'evidence': '<form method="post" action="./" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '3', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '5', 'alertRef': '10202'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '3', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '6', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '3', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '3', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '8', 'alertRef': '10061'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '3', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':

```
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '9', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '3', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '10', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '11',
'inputVector': '', 'url': 'http://ecampus.psgtech.ac.in/robots.txt', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '12', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '9', 'inputVector':
'', 'url': 'http://ecampus.psgtech.ac.in', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
```

p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '13', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '13', 'inputVector': '', 'url': 'http://ecampus.psgtech.ac.in/sitemap.xml', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '14', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '11', 'inputVector': '', 'url': 'http://ecampus.psgtech.ac.in/robots.txt', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '17', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '13', 'inputVector': '', 'url': 'http://ecampus.psgtech.ac.in/sitemap.xml', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP

Response Header Field(s)', 'param': ", 'attack': ", 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '18', 'alertRef': '10037'}

{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '9', 'inputVector': ", 'url': 'http://ecampus.psgtech.ac.in', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': ", 'attack': ", 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '19', 'alertRef': '10037'}

{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': ", 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '43', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header', 'param': 'x-frame-options', 'attack': ", 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id': '28', 'alertRef': '10020-1'}

{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '36', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/feedback/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': ", 'attack': ", 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '29', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '40', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header', 'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id': '30', 'alertRef': '10020-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '29', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/style.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '33', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '31', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/script.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '34', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '36', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/', 'tags':

{'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '35', 'alertRef': '10061'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '31', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/script.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '36', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '29', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/style.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '37', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '35', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/wowslider.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header

Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '38', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525',
'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is
missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files
this might be intended, however, the resources should be reviewed to ensure that no sensitive content
will be cached.', 'messageId': '40', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags':
{'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/
www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_T
esting/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/
cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla
.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-re
commendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with
"no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives
"public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control',
'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '39', 'alertRef':
'10015'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525',
'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is
missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files
this might be intended, however, the resources should be reviewed to ensure that no sensitive content
will be cached.', 'messageId': '43', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags':
{'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/
www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_T
esting/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/
cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla
.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-re
commendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with
"no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives
"public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control',
'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '41', 'alertRef':
'10015'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '36', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '43', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to

interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '35', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/engine1/wowslider.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '44', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '33', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '45', 'alertRef': '10038-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '29',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/style.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '46', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '31',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/script.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '49', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '43', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '50', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '59', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/icon/apple-touch-icon.jpg',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co

m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '51', 'alertRef': '10038-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '29', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/style.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '52', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '31', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/script.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '53', 'alertRef': '10037'}

{'sourceid': '3', 'other': '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: "__VIEWSTATE" "__VIEWSTATEGENERATOR"].', 'method': 'POST', 'evidence': '<form method="post" action="./" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF

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.", 'messageId': '57', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '54', 'alertRef': '10202'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '35', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/wowslider.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '56', 'alertRef': '10021'}
{'sourceid': '3', 'other': '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: "__VIEWSTATE" "__VIEWSTATEGENERATOR" "txtpwd" "TxtRollNo"].', 'method': 'GET', 'evidence':

'<form method="post" action="./FbkWfLogin.aspx" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '43', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '58', 'alertRef': '10202'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '59', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand

p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '59', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '61', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header', 'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id': '60', 'alertRef': '10020-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '35', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/wowslider.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '61', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '33', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header

Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '62', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSER\\b and was detected in the element starting with: "<script type="text/javascript">\r\n\r\n \r\n\r\n $(document).ready(function () {\r\n \r\n \r\n //", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'User', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '43', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '64', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '59', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '66', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '65', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '67', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy

mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '33', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '68', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'No links have been found while there are scripts, which is an indication that this is a modern web application.', 'method': 'GET', 'evidence': '<script src="bootstrap/js/jquery-2.1.1.min.js"></script>', 'pluginId': '10109', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1', '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.', 'messageId': '43', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {}, 'reference': '', 'solution': 'This is an informational alert and so no changes are required.', 'alert': 'Modern Web Application', 'param': '', 'attack': '', 'name': 'Modern Web Application', 'risk': 'Informational', 'id': '70', 'alertRef': '10109'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525', 'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.', 'messageId': '61', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-recommendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control', 'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '71', 'alertRef': '10015'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '65', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '73', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '59', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '74', 'alertRef': '10037'}

{'sourceid': '3', 'other': 'User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:\n\nhttps://ecampus.psgtech.ac.in/\n\nappears to include user input in: \n\na(n) [input] tag [value] attribute \n\nThe user input found was:\n__VIEWSTATEGENERATOR=71766258\n\nThe user-controlled value was:\n71766258', 'method': 'POST', 'evidence': '', 'pluginId': '10031', 'cweid': '20', 'confidence': 'Low', 'wascid': '20', '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.', 'messageId': '33', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A03': 'https://owasp.org/Top10/A03_2021-Injection/', 'CWE-20': 'https://cwe.mitre.org/data/definitions/20.html', 'OWASP_2017_A01': 'https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html', 'solution': 'Validate all input and sanitize output it before writing to any HTML attributes.', 'alert': 'User Controllable HTML Element Attribute (Potential XSS)', 'param': '__VIEWSTATEGENERATOR', 'attack': '', 'name': 'User Controllable HTML Element Attribute (Potential XSS)', 'risk': 'Informational', 'id': '76', 'alertRef': '10031'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '61', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',

'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '78', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '43', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '79', 'alertRef': '10036'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '65', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '82', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '78', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern

Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header', 'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id': '83', 'alertRef': '10020-1'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'POST', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '33', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '84', 'alertRef': '10061'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '43', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '86', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Set-Cookie: ASP.NET_SessionId', 'pluginId': '10054', 'cweid': '1275', 'confidence': 'Medium', 'wascid': '13', 'description': "A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.", 'messageId': '61', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes', 'CWE-1275': 'https://cwe.mitre.org/data/definitions/1275.html', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html'}, 'reference': 'https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site', 'solution': "Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.", 'alert': 'Cookie without SameSite Attribute', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Cookie without SameSite Attribute', 'risk': 'Low', 'id': '87', 'alertRef': '10054-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '65', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '88', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525', 'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.', 'messageId': '78', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-recommendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control', 'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '90', 'alertRef': '10015'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '80', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '91', 'alertRef': '10036'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'POST', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '33', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '92', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Set-Cookie: ASP.NET_SessionId', 'pluginId': '10011', 'cweid': '614', 'confidence': 'Medium', 'wascid': '13', 'description': 'A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.', 'messageId': '61', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-614': 'https://cwe.mitre.org/data/definitions/614.html', 'WSTG-v42-SESS-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html', 'solution': 'Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.', 'alert': 'Cookie Without Secure Flag', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Cookie Without Secure Flag', 'risk': 'Low', 'id': '94', 'alertRef': '10011'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '43', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '95', 'alertRef': '10061'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '78', 'inputVector': '', 'url':

```
'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '97', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '80', 'inputVector': '', 'url': 'htt
ps://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/sweetalert.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '98', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '57', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '99', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '81',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/w3.css', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
```

on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '101', 'alertRef': '10036'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '43', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '102', 'alertRef': '10021'}

{'sourceid': '3', 'other': '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: "__VIEWSTATE" "__VIEWSTATEGENERATOR" "txtpwd" "TxtRollNo"].', 'method': 'POST', 'evidence': '<form method="post" action="./FbkWfLogin.aspx" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '78', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati

on_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '104', 'alertRef': '10202'}
{'sourceid': '3', 'other': '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: "__EVENTARGUMENT" "__EVENTTARGET" "__EVENTVALIDATION" "__LASTFOCUS" "__VIEWSTATE" "__VIEWSTATEGENERATOR" "abcd3" "btnRefresh" "rdolst_0" "rdolst_1" "rdolst_2" "rdolst_3" "txtpwdcheck" "txtusercheck"].', 'method': 'GET', 'evidence': '<form method="post" action="./" onsubmit="javascript:return WebForm_OnSubmit();" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '61', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase:

Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '105', 'alertRef': '10202'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '80', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '106', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '81', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '107', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '85', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '108', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '43', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '109', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '87',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/psglogo.jpg', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '111', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSER\\b and was detected in the element
starting with: "<script type="text/javascript">\r\n\r\n \r\n\r\n $(document).ready(function () {\r\n \r\n \r\n
//", see evidence field for the suspicious comment/snippet.', 'method': 'POST', 'evidence': 'User',
```

'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '78', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '112', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '80', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '113', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '61', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '114', 'alertRef': '10036'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '81', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '115', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '85', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '116', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '87', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/psglogo.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '118', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '61', 'inputVector': '', 'url':

'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '119', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': 'No links have been found while there are scripts, which is an indication that this is a modern web application.', 'method': 'POST', 'evidence': '<script src="bootstrap/js/jquery-2.1.1.min.js"></script>', 'pluginId': '10109', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1', '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.', 'messageId': '78', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {}, 'reference': '', 'solution': 'This is an informational alert and so no changes are required.', 'alert': 'Modern Web Application', 'param': '', 'attack': '', 'name': 'Modern Web Application', 'risk': 'Informational', 'id': '120', 'alertRef': '10109'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '81', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '122', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '91', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/PSG.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response

Header Field', 'risk': 'Low', 'id': '123', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '85', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '124', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '87',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/psglogo.jpg', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '126', 'alertRef': '10021'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method':
'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14',
'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response
header field(s).', 'messageId': '61', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/',
'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_A
pplication_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933':
'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varun
m/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not
return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name':
'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '127', 'alertRef': '10061'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid':
'200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '78', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '128', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '93', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/psgtechlogo.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '130', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '91', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/PSG.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '131', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '85', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg', 'tags': {'OWASP_2021_A01':

'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '132', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '87', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/Images/psglogo.jpg', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '134', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '78', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '135', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '61',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A05':

'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '136', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '93', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/psgtechlogo.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '138', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '91', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/PSG.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '139', 'alertRef': '10021'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'POST', 'evidence': 'p2ghxyuo1jnhbxvbasqlufyj', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.',

'messageId': '178', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '141', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '61', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '142', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '94', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/engine1/style.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '143', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:\n\nhttps://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx\n\nappears to include user input in: \n\na(n) [input] tag [value] attribute \n\nThe user input found was:\n__VIEWSTATEGENERATOR=F20FAB24\n\nThe user-controlled value was:\nf20fab24', 'method': 'POST', 'evidence': '', 'pluginId': '10031', 'cweid': '20', 'confidence': 'Low', 'wascid': '20', '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.', 'messageId': '78', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A03': 'https://owasp.org/Top10/A03_2021-Injection/', 'CWE-20': 'https://cwe.mitre.org/data/definitions/20.html', 'OWASP_2017_A01': 'https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html'}, 'reference':

'https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html', 'solution': 'Validate all input and sanitize output it before writing to any HTML attributes.', 'alert': 'User Controllable HTML Element Attribute (Potential XSS)', 'param': '__VIEWSTATEGENERATOR', 'attack': '', 'name': 'User Controllable HTML Element Attribute (Potential XSS)', 'risk': 'Informational', 'id': '144', 'alertRef': '10031'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '93', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/psgtechlogo.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '146', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '91', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/PSG.png', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '147', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '97', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference':

'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern
Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one
of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header',
'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id':
'149', 'alertRef': '10020-1'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method':
'POST', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14',
'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response
header field(s).', 'messageId': '78', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags':
{'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933':
'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varun
m/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not
return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name':
'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '150', 'alertRef': '10061'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '94', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/engine1/style.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '151', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'p2ghxyuo1jnhbxvbasqlufyj', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '61', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '153', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '93', 'inputVector': '', 'url':

```
'https://ecampus.psgtech.ac.in/studzone2/Images/psgtechlogo.jpg', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '154', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525',
'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is
missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files
this might be intended, however, the resources should be reviewed to ensure that no sensitive content
will be cached.', 'messageId': '97', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'CWE-525':
'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/www-project-
web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Tes
ting_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/
Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla.org/en-US/d
ocs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-recommendati
ons/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with "no-cache,
no-store, must-revalidate". If an asset should be cached consider setting the directives "public,
max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control', 'attack':
'', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '156', 'alertRef': '10015'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bQUERY\\b and was detected 3 times, the first
in the element starting with: " var query = "";\r", see evidence field for the suspicious comment/snippet.',
'method': 'GET', 'evidence': 'query', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13',
'description': 'The response appears to contain suspicious comments which may help an attacker. Note:
Matches made within script blocks or files are against the entire content not only comments.',
'messageId': '114', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/WebResource.axd?d
=pynGkmcFUV13He1Qd6_TZGNy9TNFhWGKJqZkrv3qdIqNlizrIchKtzdxZ2DsVI0VfjVOw2bzbH6DIqN
yi8-0tg2&t=637475441981919477', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that
return information that may help an attacker and fix any underlying problems they refer to.', 'alert':
'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure -
Suspicious Comments', 'risk': 'Informational', 'id': '157', 'alertRef': '10027'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'POST', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence':
'Medium', 'wascid': '15', '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.", 'messageId': '78',
'inputVector': '', 'url':
```

'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '158', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '94', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/engine1/style.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '160', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '117', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/engine1/wowslider.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '161', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bSELECT\\b and was detected in the element starting with: " else if (tagName == "select") {\r", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'select', 'pluginId': '10027', 'cweid': '200', 'confidence':

```
'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may
help an attacker. Note: Matches made within script blocks or files are against the entire content not only
comments.', 'messageId': '114', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/WebRes
ource.axd?d=pynGkmcFUV13He1Qd6_TZGNy9TNFhWGKJqZkrv3qdIqNlizrIchKtzdxZ2DsVI0VfjVOw2
bzbH6DIqNyi8-0tg2&t=637475441981919477', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that
return information that may help an attacker and fix any underlying problems they refer to.', 'alert':
'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure -
Suspicious Comments', 'risk': 'Informational', 'id': '163', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '97', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '164', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '78', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '165', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '94', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/engine1/style.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '166', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '117', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/engine1/wowslider.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '168', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '114', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/WebResource.axd?d=pynGkmcFUV13He1Qd6_TZGNy9TNFhWGKJqZkrv3qdIqNlizrIchKtzdxZ2DsVI0VfjVOw2bzbH6DIqNyi8-0tg2&t=637475441981919477', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '170', 'alertRef': '10036'}
{'sourceid': '3', 'other': '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: "__VIEWSTATE" "__VIEWSTATEGENERATOR" "btnOTP" "txtnumber" "txtroll"].', 'method': 'GET', 'evidence': '<form method="post" action="./AttWfForgotPass.aspx" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a

HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '97', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '171', 'alertRef': '10202'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '118', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header', 'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id':

'174', 'alertRef': '10020-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '117', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/engine1/wowslider.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '176', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '114', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/WebResource.axd?d=pynGkmcFUV13He1Qd6_TZGNy9TNFhWGKJqZkrv3qdIqNlizrIchKtzdxZ2DsVI0VfjVOw2bzbH6DIqNyi8-0tg2&t=637475441981919477', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '177', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the element starting with: "<script>\r\n $(document).ready(function () {\r\n // alert(\'helooo\');\r\n $("#btnOTP").click(function () {\r", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'Username', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '97', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure -

Suspicious Comments', 'risk': 'Informational', 'id': '178', 'alertRef': '10027'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '117', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/engine1/wowslider.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '181', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525', 'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.', 'messageId': '118', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-recommendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control', 'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '182', 'alertRef': '10015'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '116', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech_coimbatore.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '184', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '97',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '186', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method':
'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14',
'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response
header field(s).', 'messageId': '114', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Web
Resource.axd?d=pynGkmcFUV13He1Qd6_TZGNy9TNFhWGKJqZkrv3qdIqNlizrIchKtzdxZ2DsVI0VfjV
Ow2bzbH6DIqNyi8-0tg2&t=637475441981919477', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/w
ww-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathe
ring/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933':
'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varun
m/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not
return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name':
'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '187', 'alertRef': '10061'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '118', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '189', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '116', 'inputVector': '', 'url':

```
'https://ecampus.psgtech.ac.in/data1/images/psg_tech_coimbatore.png', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '190', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '97', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '192', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '114',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/WebResource.axd?d=pynGkmcFUV13H
e1Qd6_TZGNy9TNFhWGKJqZkrv3qdIqNlizrIchKtzdxZ2DsVI0VfjVOw2bzbH6DIqNyi8-0tg2&t=6374754
41981919477', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '193', 'alertRef': '10021'}
{'sourceid': '3', 'other': '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:
"__EVENTARGUMENT" "__EVENTTARGET" "__EVENTVALIDATION" "__LASTFOCUS"
"__VIEWSTATE" "__VIEWSTATEGENERATOR" "abcd3" "btnRefresh" "rdolst_0" "rdolst_1" "rdolst_2"
```

"rdolst_3" "txtpwdcheck" "txtusercheck"].', 'method': 'POST', 'evidence': '<form method="post" action="./" onsubmit="javascript:return WebForm_OnSubmit();" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '118', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '196', 'alertRef': '10202'}

{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the element starting with: "(function(e,t){function _(e){var t=M[e]={};return v.each(e.split(y),function(e,n){t[n]=!0}),t}function H(e,n,r){if(r===t&&e.node", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'username', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '123', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/engine1/jquery.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that

return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '197', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '114', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/WebResource.axd?d=pynGkmcFUV13He1Qd6_TZGNy9TNFhWGKJqZkrv3qdIqNlizrIchKtzdxZ2DsVI0VfjVOw2bzbH6DIqNyi8-0tg2&t=637475441981919477', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '198', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '126', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.intellisense.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '201', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '97', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '202', 'alertRef': '10061'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '123', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/engine1/jquery.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '203', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '118', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '204', 'alertRef': '10036'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '97', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':

'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '205', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '126', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.intellisense.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '206', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '127', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header', 'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id': '208', 'alertRef': '10020-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '116', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech_coimbatore.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':

'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '209', 'alertRef': '10021'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'POST', 'evidence':
'p2ghxyuo1jnhbxvbasqlufyj', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '190', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '210', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '123', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/engine1/jquery.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '211', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '118', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '212', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '97', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':

'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '213', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '126', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.intellisense.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '214', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '116', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech_coimbatore.png', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '215', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525', 'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.', 'messageId': '127', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla.org/en-US/d

ocs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-recommendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control', 'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '217', 'alertRef': '10015'}
{'sourceid': '3', 'other': 'User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:\n\nhttps://ecampus.psgtech.ac.in/studzone2/\n\nappears to include user input in: \n\na(n) [input] tag [value] attribute \n\nThe user input found was:\n__VIEWSTATEGENERATOR=E64D2FFE\n\nThe user-controlled value was:\ne64d2ffe', 'method': 'POST', 'evidence': '', 'pluginId': '10031', 'cweid': '20', 'confidence': 'Low', 'wascid': '20', '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.', 'messageId': '118', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A03': 'https://owasp.org/Top10/A03_2021-Injection/', 'CWE-20': 'https://cwe.mitre.org/data/definitions/20.html', 'OWASP_2017_A01': 'https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html', 'solution': 'Validate all input and sanitize output it before writing to any HTML attributes.', 'alert': 'User Controllable HTML Element Attribute (Potential XSS)', 'param': '__VIEWSTATEGENERATOR', 'attack': '', 'name': 'User Controllable HTML Element Attribute (Potential XSS)', 'risk': 'Informational', 'id': '219', 'alertRef': '10031'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '123', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/engine1/jquery.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '220', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '127', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A05':

'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '222', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '134', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/css/responsive.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '225', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:\n\nhttps://ecampus.psgtech.ac.in/studzone2/\n\nappears to include user input in: \n\na(n) [input] tag [value] attribute \n\nThe user input found was:\ntxtpwdcheck=ZAP\n\nThe user-controlled value was:\nzap', 'method': 'POST', 'evidence': '', 'pluginId': '10031', 'cweid': '20', 'confidence': 'Low', 'wascid': '20', '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.', 'messageId': '118', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A03': 'https://owasp.org/Top10/A03_2021-Injection/', 'CWE-20': 'https://cwe.mitre.org/data/definitions/20.html', 'OWASP_2017_A01': 'https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html', 'solution': 'Validate all input and sanitize output it before writing to any HTML attributes.', 'alert': 'User Controllable HTML Element Attribute (Potential XSS)', 'param': 'txtpwdcheck', 'attack': '', 'name': 'User Controllable HTML Element Attribute (Potential XSS)', 'risk': 'Informational', 'id': '226', 'alertRef': '10031'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '123', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/engine1/jquery.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':

```
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '227', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '135', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '229', 'alertRef': '10036'}
{'sourceid': '3', 'other': '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: "__EVENTARGUMENT" "__EVENTTARGET" "__EVENTVALIDATION" "__LASTFOCUS" "__VIEWSTATE" "__VIEWSTATEGENERATOR" "abcd3" "btnRefresh" "rdolst_0" "rdolst_1" "rdolst_2" "rdolst_3" "txtpwdcheck" "txtusercheck" ].', 'method': 'GET', 'evidence': '<form method="post" action="./AttWfLoginPage.aspx" onsubmit="javascript:return WebForm_OnSubmit();" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '127', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheats
```

heets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '231', 'alertRef': '10202'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '134', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/css/responsive.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '232', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '140', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '233', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:\n\nhttps://ecampus.psgtech.ac.in/studzone2/\n\nappears to include user input in: \n\na(n) [input] tag [value] attribute \n\nThe user input found was:\ntxtusercheck=ZAP\n\nThe user-controlled value

was:\nzap', 'method': 'POST', 'evidence': '', 'pluginId': '10031', 'cweid': '20', 'confidence': 'Low', 'wascid': '20', '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.', 'messageId': '118', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A03': 'https://owasp.org/Top10/A03_2021-Injection/', 'CWE-20': 'https://cwe.mitre.org/data/definitions/20.html', 'OWASP_2017_A01': 'https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html', 'solution': 'Validate all input and sanitize output it before writing to any HTML attributes.', 'alert': 'User Controllable HTML Element Attribute (Potential XSS)', 'param': 'txtusercheck', 'attack': '', 'name': 'User Controllable HTML Element Attribute (Potential XSS)', 'risk': 'Informational', 'id': '234', 'alertRef': '10031'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '135', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '236', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'CVE-2020-11023\nCVE-2020-11022\nCVE-2015-9251\nCVE-2019-11358\nCVE-2020-7656\nCVE-2012-6708\n', 'method': 'GET', 'evidence': '/*! jQuery v1.8.3', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library jquery, version 1.8.3 is vulnerable.', 'messageId': '123', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/engine1/jquery.js', 'tags': {'CVE-2020-11023': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11023', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2020-11022': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11022', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CVE-2015-9251': 'https://nvd.nist.gov/vuln/detail/CVE-2015-9251', 'CVE-2019-11358': 'https://nvd.nist.gov/vuln/detail/CVE-2019-11358', 'CVE-2020-7656': 'https://nvd.nist.gov/vuln/detail/CVE-2020-7656', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html', 'CVE-2012-6708': 'https://nvd.nist.gov/vuln/detail/CVE-2012-6708'}, 'reference': 'https://nvd.nist.gov/vuln/detail/CVE-2012-6708\nhttps://github.com/jquery/jquery/issues/2432\nhttp://research.insecurelabs.org/jquery/test/\nhttps://nvd.nist.gov/vuln/detail/CVE-2019-11358\nhttps://github.com/advisories/GHSA-rmxg-73gg-4p98\nhttps://bugs.jquery.com/ticket/11974\nhttps://github.com/jquery/jquery.com/issues/162\nhttps://nvd.nist.gov/vuln/detail/CVE-2020-7656\nhttp://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/\nhttp://bugs.jquery.com/ticket/11290\nhttps://blog.jquery.com/2019/04/10/jquery-3-4-0-released/\nhttps://nvd.nist.gov/vuln/detail/CVE-2015-9251\nhttps://github.com/advisories/GHSA-q4m3-2j7h-f7xw\nhttps://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b\nhttps://blog.jquery.com/2020/04/10/jquery-3-5-0-released/\n', 'solution': 'Please upgrade to the latest version of jquery.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '238', 'alertRef': '10003'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy

mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '140', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '239', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '134',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/css/responsive.css', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '240', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '127',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '241', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'User-controlled HTML attribute values were found. Try injecting special
characters to see if XSS might be possible. The page at the following

URL:\n\nhttps://ecampus.psgtech.ac.in/studzone2/\n\nappears to include user input in: \n\na(n) [input] tag [value] attribute \n\nThe user input found was:\nbtnRefresh=Refresh\n\nThe user-controlled value was:\nrefresh', 'method': 'POST', 'evidence': '', 'pluginId': '10031', 'cweid': '20', 'confidence': 'Low', 'wascid': '20', '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.', 'messageId': '118', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A03': 'https://owasp.org/Top10/A03_2021-Injection/', 'CWE-20': 'https://cwe.mitre.org/data/definitions/20.html', 'OWASP_2017_A01': 'https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html', 'solution': 'Validate all input and sanitize output it before writing to any HTML attributes.', 'alert': 'User Controllable HTML Element Attribute (Potential XSS)', 'param': 'btnRefresh', 'attack': '', 'name': 'User Controllable HTML Element Attribute (Potential XSS)', 'risk': 'Informational', 'id': '242', 'alertRef': '10031'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '135', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '245', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '134', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/css/responsive.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '247', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '127', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '248', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '140', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '249', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'POST', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '118', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '250', 'alertRef': '10061'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '135', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga

thering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '251', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '141',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.js', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '253', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method':
'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14',
'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response
header field(s).', 'messageId': '127', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://
owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Inform
ation_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933':
'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varun
m/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not
return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name':
'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '255', 'alertRef': '10061'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'POST', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence':
'Medium', 'wascid': '15', '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.", 'messageId': '118',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt

ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': ", 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '258', 'alertRef': '10021'}

{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': ", 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '141', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': ", 'attack': ", 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '260', 'alertRef': '10035-1'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': ", 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '127', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': ", 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '262', 'alertRef': '10021'}

{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '142', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/modernizr-2.5.3.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati

on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '264', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '143', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/_references.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '265', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '118', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '266', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '141', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit

y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '268', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '144', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '269', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '127', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '270', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '142', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/modernizr-2.5.3.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce

Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '271', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '143', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/_references.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '272', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '144', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '274', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=ZAP\npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST', 'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.', 'messageId': '118', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request Identified', 'risk': 'Informational', 'id': '275', 'alertRef': '10111'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '143', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/_references.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':

'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '278', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '142', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/modernizr-2.5.3.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '279', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '144', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '282', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '145', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand

p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '283', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '145', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '288', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:\n\nhttps://ecampus.psgtech.ac.in/studzone2/\n\nappears to include user input in: \n\na(n) [input] tag [value] attribute \n\nThe user input found was:\nabcd3=Login\n\nThe user-controlled value was:\nlogin', 'method': 'POST', 'evidence': '', 'pluginId': '10031', 'cweid': '20', 'confidence': 'Low', 'wascid': '20', '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.', 'messageId': '129', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A03': 'https://owasp.org/Top10/A03_2021-Injection/', 'CWE-20': 'https://cwe.mitre.org/data/definitions/20.html', 'OWASP_2017_A01': 'https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html', 'solution': 'Validate all input and sanitize output it before writing to any HTML attributes.', 'alert': 'User Controllable HTML Element Attribute (Potential XSS)', 'param': 'abcd3', 'attack': '', 'name': 'User Controllable HTML Element Attribute (Potential XSS)', 'risk': 'Informational', 'id': '290', 'alertRef': '10031'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '145', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '291', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '149', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '298', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '151', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header', 'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id': '299', 'alertRef': '10020-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '155', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/images/psg-logo.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '300', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '149', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '301', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '155', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/images/psg-logo.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '302', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '160', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/lock.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '303', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525', 'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.', 'messageId': '151', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'CWE-525':

'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-recommendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control', 'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '304', 'alertRef': '10015'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '157', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '305', 'alertRef': '10036'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '155', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/images/psg-logo.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '306', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '149',
'inputVector': ", 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/ecampus.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': ", 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '307', 'alertRef': '10021'}
{'sourceid': '3', 'other': ", 'method': 'POST', 'evidence': ", 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '151', 'inputVector': ", 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': ", 'attack': ", 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '308', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': ", 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '160', 'inputVector': ", 'url':
'https://ecampus.psgtech.ac.in/studzone2/Images/lock.png', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': ", 'attack': ",
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '309', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bSELECT\\b and was detected in the element
starting with: " if (control.tagName != "INPUT" && control.tagName != "TEXTAREA" &&
control.tagName != "SELECT") {\r", see evidence field for the suspicious comment/snippet.', 'method':

'GET', 'evidence': 'SELECT', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13',
'description': 'The response appears to contain suspicious comments which may help an attacker. Note:
Matches made within script blocks or files are against the entire content not only comments.',
'messageId': '153', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?
d=1HpV3OVB0CaEXoaafcqmht5lVuxEcIp-gYUAJpTK7_CvslKPIRWHcstuT3XAFJ7K5rLDcyyKMAznK
HhH_GiqgweLa-UJ-VUJ8g9rDkxlvFfQf3rGv1wRCXKGHgKDfEw3EU6ZxSBgg6F6G1ZM-6nuGA2&t=3
ee86f5f', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leaka
ge', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that
return information that may help an attacker and fix any underlying problems they refer to.', 'alert':
'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure -
Suspicious Comments', 'risk': 'Informational', 'id': '310', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '157', 'inputVector': '', 'url': 'h
ttps://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/js/sweetalert.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '311', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '149', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/ecampus.css',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '312', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '155', 'inputVector': '', 'url':

'https://ecampus.psgtech.ac.in/studzone2/images/psg-logo.png', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '313', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bFROM\\b and was detected in the element starting with: "!function (t, e) { "object" == typeof exports && "object" == typeof module ? module.exports = e() : "function" == typeof define ", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'from', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '150', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '314', 'alertRef': '10027'}
{'sourceid': '3', 'other': '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: "__VIEWSTATE" "__VIEWSTATEGENERATOR" "btnOTP" "txtnumber" "txtroll"].', 'method': 'POST', 'evidence': '<form method="post" action="./AttWfForgotPass.aspx" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '151', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352':

'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '315', 'alertRef': '10202'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '160', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/lock.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '316', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '153', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=1HpV3OVB0CaEXoaafcqmht5lVuxEcIp-gYUAJpTK7_CvslKPIRWHcstuT3XAFJ7K5rLDcyyKMAznKHhH_GiqgweLa-UJ-VUJ8g9rDkxlvFfQf3rGv1wRCXKGHgKDfEw3EU6ZxSBgg6F6G1ZM-6nuGA2&t=3ee86f5f', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand

p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '317', 'alertRef': '10036'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '157', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '318', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '150', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '319', 'alertRef': '10036'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'p2ghxyuo1jnhbxvbasqlufyj', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '203', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKxUvgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriYg

Reyv3ohx7-ei-o01&t=10c151ff', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '320', 'alertRef': '10112'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '160', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/lock.png', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '322', 'alertRef': '10037'}

{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the element starting with: "<script>\r\n $(document).ready(function () {\r\n // alert(\'helooo\');\r\n $("#btnOTP").click(function () {\r", see evidence field for the suspicious comment/snippet.', 'method': 'POST', 'evidence': 'Username', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '151', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '323', 'alertRef': '10027'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '153', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=1HpV3OVB0CaEXoaafcqmht5lVuxEcIp-gYUAJpTK7_CvslKPIRWHcstuT3XAFJ7K5rLDcyyKMAznKHhH_GiqgweLa-UJ-VUJ8g9rDkxlvFfQf3rGv1wRCXKGHgKDfEw3EU6ZxSBgg6F6G1ZM-6nuGA2&t=3ee86f5f', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce

Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': ", 'attack': ", 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '324', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '157', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': ", 'attack': ", 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '325', 'alertRef': '10037'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': ", 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '150', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': ", 'attack': ", 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '326', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSER\\b and was detected 10 times, the first in the element starting with: " * (this is what the user calls)", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'user', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '158', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert-dev.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': ", 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': ", 'attack': ", 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '329', 'alertRef': '10027'}
{'sourceid': '3', 'other': ", 'method': 'POST', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '151', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '330', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '153', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=1HpV3OVB0CaEXoaafcqmht5lVuxEcIp-gYUAJpTK7_CvslKPIRWHcstuT3XAFJ7K5rLDcyyKMAznKHhH_GiqgweLa-UJ-VUJ8g9rDkxlvFfQf3rGv1wRCXKGHgKDfEw3EU6ZxSBgg6F6G1ZM-6nuGA2&t=3ee86f5f', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '331', 'alertRef': '10061'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '150', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '332', 'alertRef': '10021'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bFROM\\b and was detected 2 times, the first in the element starting with: " * Use argument if defined or default value from params object otherwise.",

see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'from', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '158', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert-dev.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '333', 'alertRef': '10027'}

{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '151', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '336', 'alertRef': '10035-1'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '153', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=1HpV3OVB0CaEXoaafcqmht5lVuxEcIp-gYUAJpTK7_CvslKPIRWHcstuT3XAFJ7K5rLDcyyKMAznKHhH_GiqgweLa-UJ-VUJ8g9rDkxlvFfQf3rGv1wRCXKGHgKDfEw3EU6ZxSBgg6F6G1ZM-6nuGA2&t=3ee86f5f', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '337', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '150', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '338', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bWHERE\\b and was detected 2 times, the first in the element starting with: " * Remember state in cases where opening and handling a modal will fiddle with it.", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'where', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '158', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert-dev.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '339', 'alertRef': '10027'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bDB\\b and was detected 2 times, the first in the element starting with: "!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.docu", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'db', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '164', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '341', 'alertRef': '10027'}
{'sourceid': '3', 'other': 'User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:\n\nhttps://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx\n\nappears to include user input in: \n\na(n) [input] tag [value] attribute \n\nThe user input found was:\n__VIEWSTATEGENERATOR=7A2C63D2\n\nThe user-controlled value was:\n7a2c63d2', 'method': 'POST', 'evidence': '', 'pluginId': '10031', 'cweid': '20', 'confidence': 'Low', 'wascid': '20',

'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.', 'messageId': '151', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A03': 'https://owasp.org/Top10/A03_2021-Injection/', 'CWE-20': 'https://cwe.mitre.org/data/definitions/20.html', 'OWASP_2017_A01': 'https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html', 'solution': 'Validate all input and sanitize output it before writing to any HTML attributes.', 'alert': 'User Controllable HTML Element Attribute (Potential XSS)', 'param': '__VIEWSTATEGENERATOR', 'attack': '', 'name': 'User Controllable HTML Element Attribute (Potential XSS)', 'risk': 'Informational', 'id': '342', 'alertRef': '10031'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '153', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=1HpV3OVB0CaEXoaafcqmht5lVuxEcIp-gYUAJpTK7_CvslKPIRWHcstuT3XAFJ7K5rLDcyyKMAznKHhH_GiqgweLa-UJ-VUJ8g9rDkxlvFfQf3rGv1wRCXKGHgKDfEw3EU6ZxSBgg6F6G1ZM-6nuGA2&t=3ee86f5f', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '343', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the element starting with: "},removeAttr:function(a,b){var c,d,e=0,f=b&&b.match(E);if(f&&1===a.nodeType)while(c=f[e++])d=n.propFix[c]||c,n.expr.match.bool.t", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'username', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '164', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '344', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '158',

'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert-dev.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '345', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'POST', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '151', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '347', 'alertRef': '10061'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '166', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '348', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '164', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati

```
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '350', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '158', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert-dev.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '351', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'POST', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence':
'Medium', 'wascid': '15', '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.", 'messageId': '151',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '352', 'alertRef': '10021'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the
element starting with: "(function(e,t){function _(e){var t=M[e]={};return
v.each(e.split(y),function(e,n){t[n]=!0}),t}function H(e,n,r){if(r===t&&e.node", see evidence field for the
suspicious comment/snippet.', 'method': 'GET', 'evidence': 'username', 'pluginId': '10027', 'cweid': '200',
'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments
which may help an attacker. Note: Matches made within script blocks or files are against the entire
content not only comments.', 'messageId': '165', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/engine1/jquery.js', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.or
```

g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '353', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '166', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '356', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '164', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '358', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '151', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"

HTTP Response Header Field(s)', 'risk': 'Low', 'id': '359', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '165', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/jquery.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '360', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '170', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header', 'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id': '362', 'alertRef': '10020-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '166', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '363', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '158',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert-dev.js', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '364', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '165', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/engine1/jquery.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '366', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '164',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstra
p/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
```

'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '369', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '166', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '370', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '158', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert-dev.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '371', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '164', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',

'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '373', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525',
'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is
missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files
this might be intended, however, the resources should be reviewed to ensure that no sensitive content
will be cached.', 'messageId': '170', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'CWE-525':
'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/www-project-
web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Tes
ting_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/
Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla.org/en-US/d
ocs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-recommendati
ons/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with "no-cache,
no-store, must-revalidate". If an asset should be cached consider setting the directives "public,
max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control', 'attack':
'', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '375', 'alertRef': '10015'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '165',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/jquery.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '376', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '170', 'inputVector': '', 'url':

```
'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '378', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '165', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/engine1/jquery.js', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '379', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'CVE-2020-11023\nCVE-2020-11022\nCVE-2015-9251\nCVE-2019-11358\n',
'method': 'GET', 'evidence': 'jquery-2.1.1.min.js', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium',
'wascid': '-1', 'description': 'The identified library jquery, version 2.1.1 is vulnerable.', 'messageId': '164',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstra
p/js/jquery-2.1.1.min.js', 'tags': {'CVE-2020-11023': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11023',
'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_
Known_Vulnerabilities.html', 'CVE-2020-11022': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11022',
'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/',
'CVE-2015-9251': 'https://nvd.nist.gov/vuln/detail/CVE-2015-9251', 'CVE-2019-11358':
'https://nvd.nist.gov/vuln/detail/CVE-2019-11358', 'CWE-829':
'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/jquery/jquery/issues/24
32\nhttp://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/\nhttp://research.insecurelabs.org/
jquery/test/\nhttps://blog.jquery.com/2019/04/10/jquery-3-4-0-released/\nhttps://nvd.nist.gov/vuln/detail/
CVE-2019-11358\nhttps://github.com/advisories/GHSA-rmxg-73gg-4p98\nhttps://nvd.nist.gov/vuln/deta
il/CVE-2015-9251\nhttps://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd08086
19b1b\nhttps://bugs.jquery.com/ticket/11974\nhttps://github.com/jquery/jquery.com/issues/162\nhttps://
blog.jquery.com/2020/04/10/jquery-3-5-0-released/\n', 'solution': 'Please upgrade to the latest version of
jquery.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk':
'Medium', 'id': '381', 'alertRef': '10003'}
{'sourceid': '3', 'other': 'CVE-2018-14041\nCVE-2019-8331\nCVE-2018-20677\nCVE-2018-20676\nCV
E-2018-14042\nCVE-2016-10735\n', 'method': 'GET', 'evidence': '* Bootstrap v3.3.7', 'pluginId': '10003',
'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library bootstrap, version
3.3.7 is vulnerable.', 'messageId': '166', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S
(mltvpupbefxv01gpxzk00x1g))/bootstrap/js/bootstrap.min.js', 'tags': {'CVE-2018-14041':
'https://nvd.nist.gov/vuln/detail/CVE-2018-14041', 'CVE-2019-8331':
```

'https://nvd.nist.gov/vuln/detail/CVE-2019-8331', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2018-20677': 'https://nvd.nist.gov/vuln/detail/CVE-2018-20677', 'CVE-2018-20676': 'https://nvd.nist.gov/vuln/detail/CVE-2018-20676', 'CVE-2018-14042': 'https://nvd.nist.gov/vuln/detail/CVE-2018-14042', 'CVE-2016-10735': 'https://nvd.nist.gov/vuln/detail/CVE-2016-10735', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/twbs/bootstrap/issues/28236\nhttps://github.com/advisories/GHSA-pj7m-g53m-7638\nhttps://github.com/twbs/bootstrap/issues/20184\nhttps://github.com/advisories/GHSA-ph58-4vrj-w6hr\nhttps://github.com/twbs/bootstrap/issues/20631\nhttps://github.com/advisories/GHSA-4p24-vmcr-4gqj\nhttps://github.com/advisories/GHSA-9v3m-8fp8-mj99\nhttps://nvd.nist.gov/vuln/detail/CVE-2018-20676\n', 'solution': 'Please upgrade to the latest version of bootstrap.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '382', 'alertRef': '10003'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bDEBUG\\b and was detected in the element starting with: "// Name: MicrosoftAjaxWebForms.debug.js\r", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'debug', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '171', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=geiJw278ELCE4oVrRV2zHxl4wPiCyAyFHHfDFzBwX9Hp7XbtV3NCf3xuCpzPTnIRW2dJvayOXQqOoSXyt8im1TzMRVB0IuHKFJU24PVx4BTHjdtmWWkIrjaXmOc8s0R8UPDzpkdImHC-ll2ojyANip2Z-suFTjJXCyu_H-il4yDEOHJiEVBhwuI32VFkf50c0&t=10c151ff', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '383', 'alertRef': '10027'}
{'sourceid': '3', 'other': '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: "__EVENTARGUMENT" "__EVENTTARGET" "__EVENTVALIDATION" "__LASTFOCUS" "__VIEWSTATE" "__VIEWSTATEGENERATOR" "abcd3" "btnRefresh" "rdolst_0" "rdolst_1" "rdolst_2" "rdolst_3" "txtpwdcheck" "txtusercheck"].', 'method': 'POST', 'evidence': '<form method="post" action="./AttWfLoginPage.aspx" onsubmit="javascript:return WebForm_OnSubmit();" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.",

```
'messageId': '170', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Mana
gement_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05':
'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352':
'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheats
heets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitio
ns/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does
not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor
example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase:
Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF
defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and
Design\nGenerate 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).\nNote that this can be
bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management
control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request
that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF
Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '385',
'alertRef': '10202'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bQUERY\\b and was detected 3 times, the first
in the element starting with: " var domain = "", query = "", queryIndex = action.indexOf(\'?\');\r", see
evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'query', 'pluginId':
'10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain
suspicious comments which may help an attacker. Note: Matches made within script blocks or files are
against the entire content not only comments.', 'messageId': '171', 'inputVector': '', 'url': 'https://ecampus
.psgtech.ac.in/studzone2/ScriptResource.axd?d=geiJw278ELCE4oVrRV2zHxl4wPiCyAyFHHfDFzBwX
9Hp7XbtV3NCf3xuCpzPTnIRW2dJvayOXQqOoSXyt8im1TzMRVB0IuHKFJU24PVx4BTHjdtmWWkIrja
XmOc8s0R8UPDzpkdImHC-ll2ojyANip2Z-suFTjJXCyu_H-il4yDEOHJiEVBhwuI32VFkf50c0&t=10c151f
f', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leaka
ge', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that
return information that may help an attacker and fix any underlying problems they refer to.', 'alert':
'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure -
Suspicious Comments', 'risk': 'Informational', 'id': '388', 'alertRef': '10027'}
{'sourceid': '3', 'other': 'CVE-2020-11023\nCVE-2020-11022\nCVE-2015-9251\nCVE-2019-11358\nCV
E-2020-7656\nCVE-2012-6708\n', 'method': 'GET', 'evidence': '/*! jQuery v1.8.3', 'pluginId': '10003',
'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library jquery, version
1.8.3 is vulnerable.', 'messageId': '165', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/engine1/jquery.js', 'tags': {'CVE-2020-11023':
'https://nvd.nist.gov/vuln/detail/CVE-2020-11023', 'OWASP_2017_A09': 'https://owasp.org/www-project
-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2020-11022':
'https://nvd.nist.gov/vuln/detail/CVE-2020-11022', 'OWASP_2021_A06':
'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CVE-2015-9251':
'https://nvd.nist.gov/vuln/detail/CVE-2015-9251', 'CVE-2019-11358':
'https://nvd.nist.gov/vuln/detail/CVE-2019-11358', 'CVE-2020-7656':
```

'https://nvd.nist.gov/vuln/detail/CVE-2020-7656', 'CWE-829':
'https://cwe.mitre.org/data/definitions/829.html', 'CVE-2012-6708':
'https://nvd.nist.gov/vuln/detail/CVE-2012-6708'}, 'reference': 'https://nvd.nist.gov/vuln/detail/CVE-2012-
6708\nhttps://github.com/jquery/jquery/issues/2432\nhttp://research.insecurelabs.org/jquery/test/\nhttps
://nvd.nist.gov/vuln/detail/CVE-2019-11358\nhttps://github.com/advisories/GHSA-rmxg-73gg-4p98\nhtt
ps://bugs.jquery.com/ticket/11974\nhttps://github.com/jquery/jquery.com/issues/162\nhttps://nvd.nist.go
v/vuln/detail/CVE-2020-7656\nhttp://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/\nhttp://
bugs.jquery.com/ticket/11290\nhttps://blog.jquery.com/2019/04/10/jquery-3-4-0-released/\nhttps://nvd.n
ist.gov/vuln/detail/CVE-2015-9251\nhttps://github.com/advisories/GHSA-q4m3-2j7h-f7xw\nhttps://githu
b.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b\nhttps://blog.jquery.com/
2020/04/10/jquery-3-5-0-released/\n', 'solution': 'Please upgrade to the latest version of jquery.', 'alert':
'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '389',
'alertRef': '10003'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bSELECT\\b and was detected in the element
starting with: " else if (tagName === \'SELECT\') {\r", see evidence field for the suspicious
comment/snippet.', 'method': 'GET', 'evidence': 'SELECT', 'pluginId': '10027', 'cweid': '200', 'confidence':
'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may
help an attacker. Note: Matches made within script blocks or files are against the entire content not only
comments.', 'messageId': '171', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptRe
source.axd?d=geiJw278ELCE4oVrRV2zHxl4wPiCyAyFHHfDFzBwX9Hp7XbtV3NCf3xuCpzPTnIRW2d
JvayOXQqOoSXyt8im1TzMRVB0IuHKFJU24PVx4BTHjdtmWWkIrjaXmOc8s0R8UPDzpkdImHC-ll2ojy
ANip2Z-suFTjJXCyu_H-il4yDEOHJiEVBhwuI32VFkf50c0&t=10c151ff', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that
return information that may help an attacker and fix any underlying problems they refer to.', 'alert':
'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure -
Suspicious Comments', 'risk': 'Informational', 'id': '393', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid':
'200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '170',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '395', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bFROM\\b and was detected 2 times, the first
in the element starting with: ""PRM_ServerError":"An unknown error occurred while processing the
request on the server. The status code returned from the serve", see evidence field for the suspicious
comment/snippet.', 'method': 'GET', 'evidence': 'from', 'pluginId': '10027', 'cweid': '200', 'confidence':
'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may
help an attacker. Note: Matches made within script blocks or files are against the entire content not only

comments.', 'messageId': '171', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=geiJw278ELCE4oVrRV2zHxl4wPiCyAyFHHfDFzBwX9Hp7XbtV3NCf3xuCpzPTnIRW2dJvayOXQqOoSXyt8im1TzMRVB0IuHKFJU24PVx4BTHjdtmWWkIrjaXmOc8s0R8UPDzpkdImHC-ll2ojyANip2Z-suFTjJXCyu_H-il4yDEOHJiEVBhwuI32VFkf50c0&t=10c151ff', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '400', 'alertRef': '10027'}

{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '170', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '401', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '171', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=geiJw278ELCE4oVrRV2zHxl4wPiCyAyFHHfDFzBwX9Hp7XbtV3NCf3xuCpzPTnIRW2dJvayOXQqOoSXyt8im1TzMRVB0IuHKFJU24PVx4BTHjdtmWWkIrjaXmOc8s0R8UPDzpkdImHC-ll2ojyANip2Z-suFTjJXCyu_H-il4yDEOHJiEVBhwuI32VFkf50c0&t=10c151ff', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '406', 'alertRef': '10036'}

{'sourceid': '3', 'other': 'User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:\n\nhttps://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx\n\nappears to include user input in: \n\na(n) [input] tag [value] attribute \n\nThe user input found was:\n__VIEWSTATEGENERATOR=E64D2FFE\n\nThe user-controlled value was:\ne64d2ffe', 'method': 'POST', 'evidence': '', 'pluginId': '10031', 'cweid': '20', 'confidence': 'Low', 'wascid': '20', '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.', 'messageId': '170', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A03': 'https://owasp.org/Top10/A03_2021-Injection/', 'CWE-20': 'https://cwe.mitre.org/data/definitions/20.html', 'OWASP_2017_A01': 'https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html', 'solution': 'Validate all input and sanitize output it before writing to any HTML attributes.', 'alert': 'User Controllable HTML Element Attribute (Potential XSS)', 'param': '__VIEWSTATEGENERATOR', 'attack': '', 'name': 'User Controllable HTML Element Attribute (Potential XSS)', 'risk': 'Informational', 'id': '410', 'alertRef': '10031'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '171', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=geiJw278ELCE4oVrRV2zHxl4wPiCyAyFHHfDFzBwX9Hp7XbtV3NCf3xuCpzPTnIRW2dJvayOXQqOoSXyt8im1TzMRVB0IuHKFJU24PVx4BTHjdtmWWkIrjaXmOc8s0R8UPDzpkdImHC-ll2ojyANip2Z-suFTjJXCyu_H-il4yDEOHJiEVBhwuI32VFkf50c0&t=10c151ff', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '413', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:\n\nhttps://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx\n\nappears to include user input in: \n\na(n) [input] tag [value] attribute \n\nThe user input found was:\ntxtpwdcheck=ZAP\n\nThe user-controlled value was:\nzap', 'method': 'POST', 'evidence': '', 'pluginId': '10031', 'cweid': '20', 'confidence': 'Low', 'wascid': '20', '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.', 'messageId': '170', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A03': 'https://owasp.org/Top10/A03_2021-Injection/', 'CWE-20': 'https://cwe.mitre.org/data/definitions/20.html', 'OWASP_2017_A01': 'https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html', 'solution': 'Validate all input and sanitize output it before writing to any HTML attributes.', 'alert': 'User Controllable HTML Element Attribute (Potential XSS)', 'param': 'txtpwdcheck', 'attack': '', 'name': 'User Controllable HTML Element Attribute (Potential XSS)', 'risk': 'Informational', 'id': '415', 'alertRef': '10031'}
{'sourceid': '3', 'other': 'User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:\n\nhttps://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx\n\nappears to include user input in: \n\na(n) [input] tag [value] attribute \n\nThe user input found was:\ntxtusercheck=ZAP\n\nThe user-controlled value was:\nzap', 'method': 'POST', 'evidence': '', 'pluginId': '10031', 'cweid': '20', 'confidence': 'Low', 'wascid': '20', '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.', 'messageId': '170', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A03':
'https://owasp.org/Top10/A03_2021-Injection/', 'CWE-20':
'https://cwe.mitre.org/data/definitions/20.html', 'OWASP_2017_A01':
'https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html'}, 'reference':
'https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html', 'solution':
'Validate all input and sanitize output it before writing to any HTML attributes.', 'alert': 'User Controllable
HTML Element Attribute (Potential XSS)', 'param': 'txtusercheck', 'attack': '', 'name': 'User Controllable
HTML Element Attribute (Potential XSS)', 'risk': 'Informational', 'id': '420', 'alertRef': '10031'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method':
'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14',
'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response
header field(s).', 'messageId': '171', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scri
ptResource.axd?d=geiJw278ELCE4oVrRV2zHxl4wPiCyAyFHHfDFzBwX9Hp7XbtV3NCf3xuCpzPTnIR
W2dJvayOXQqOoSXyt8im1TzMRVB0IuHKFJU24PVx4BTHjdtmWWkIrjaXmOc8s0R8UPDzpkdImHC-ll
2ojyANip2Z-suFTjJXCyu_H-il4yDEOHJiEVBhwuI32VFkf50c0&t=10c151ff', 'tags':
{'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933':
'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varun
m/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not
return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name':
'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '424', 'alertRef': '10061'}
{'sourceid': '3', 'other': 'User-controlled HTML attribute values were found. Try injecting special
characters to see if XSS might be possible. The page at the following
URL:\n\nhttps://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx\n\nappears to include user
input in: \n\na(n) [input] tag [value] attribute \n\nThe user input found was:\nbtnRefresh=Refresh\n\nThe
user-controlled value was:\nrefresh', 'method': 'POST', 'evidence': '', 'pluginId': '10031', 'cweid': '20',
'confidence': 'Low', 'wascid': '20', '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.', 'messageId': '170', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A03':
'https://owasp.org/Top10/A03_2021-Injection/', 'CWE-20':
'https://cwe.mitre.org/data/definitions/20.html', 'OWASP_2017_A01':
'https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html'}, 'reference':
'https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html', 'solution':
'Validate all input and sanitize output it before writing to any HTML attributes.', 'alert': 'User Controllable
HTML Element Attribute (Potential XSS)', 'param': 'btnRefresh', 'attack': '', 'name': 'User Controllable
HTML Element Attribute (Potential XSS)', 'risk': 'Informational', 'id': '426', 'alertRef': '10031'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '171',
```

'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=geiJw278ELCE4oVrRV2zHxl4wPiCyAyFHHfDFzBwX9Hp7XbtV3NCf3xuCpzPTnIRW2dJvayOXQqOoSXyt8im1TzMRVB0IuHKFJU24PVx4BTHjdtmWWkIrjaXmOc8s0R8UPDzpkdImHC-ll2ojyANip2Z-suFTjJXCyu_H-il4yDEOHJiEVBhwuI32VFkf50c0&t=10c151ff', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '430', 'alertRef': '10021'}

{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'POST', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '170', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '436', 'alertRef': '10061'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '171', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=geiJw278ELCE4oVrRV2zHxl4wPiCyAyFHHfDFzBwX9Hp7XbtV3NCf3xuCpzPTnIRW2dJvayOXQqOoSXyt8im1TzMRVB0IuHKFJU24PVx4BTHjdtmWWkIrjaXmOc8s0R8UPDzpkdImHC-ll2ojyANip2Z-suFTjJXCyu_H-il4yDEOHJiEVBhwuI32VFkf50c0&t=10c151ff', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '437', 'alertRef': '10037'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'POST', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence':

'Medium', 'wascid': '15', '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.", 'messageId': '170', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '441', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'POST', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '170', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '446', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bLATER\\b and was detected 8 times, the first in the element starting with: "// Give the init function the jQuery prototype for later instantiation\r", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'later', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '172', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '452', 'alertRef': '10027'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bBUG\\b and was detected 9 times, the first in the element starting with: "\t\t// hidden; don safety goggles and see bug #4512 for more information).\r", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'bug', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain

```
suspicious comments which may help an attacker. Note: Matches made within script blocks or files are
against the entire content not only comments.', 'messageId': '172', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that
return information that may help an attacker and fix any underlying problems they refer to.', 'alert':
'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure -
Suspicious Comments', 'risk': 'Informational', 'id': '456', 'alertRef': '10027'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=ZAP\npasswordParam=txtpwdcheck\nref
erer=https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'method': 'POST', 'evidence':
'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', '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.', 'messageId': '170', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/', 'solution': 'This is an
informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Authentication
Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request Identified', 'risk':
'Informational', 'id': '458', 'alertRef': '10111'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bBUGS\\b and was detected 3 times, the first
in the element starting with: "\t\t// discovered by ChrisS here:
http://bugs.jquery.com/ticket/12282#comment:15\r", see evidence field for the suspicious
comment/snippet.', 'method': 'GET', 'evidence': 'bugs', 'pluginId': '10027', 'cweid': '200', 'confidence':
'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may
help an attacker. Note: Matches made within script blocks or files are against the entire content not only
comments.', 'messageId': '172', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that
return information that may help an attacker and fix any underlying problems they refer to.', 'alert':
'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure -
Suspicious Comments', 'risk': 'Informational', 'id': '461', 'alertRef': '10027'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected 4 times, the
first in the element starting with: "\t\tusername: null,\r", see evidence field for the suspicious
comment/snippet.', 'method': 'GET', 'evidence': 'username', 'pluginId': '10027', 'cweid': '200',
'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments
which may help an attacker. Note: Matches made within script blocks or files are against the entire
content not only comments.', 'messageId': '172', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that
return information that may help an attacker and fix any underlying problems they refer to.', 'alert':
'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure -
```

Suspicious Comments', 'risk': 'Informational', 'id': '465', 'alertRef': '10027'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bQUERY\\b and was detected in the element starting with: "//key/values into a query string\r", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'query', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '172', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '471', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '182', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '473', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSER\\b and was detected 4 times, the first in the element starting with: "\t// cache in order to avoid key collisions between internal data and user-defined\r", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'user', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '172', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '478', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '182', 'inputVector': '', 'url': 'h

ttps://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '480', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': 'The following pattern was used: \\bSELECT\\b and was detected 22 times, the first in the element starting with: "\t\tinput, select, fragment,\r", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'select', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '172', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '486', 'alertRef': '10027'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '182', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '493', 'alertRef': '10021'}

{'sourceid': '3', 'other': 'The following pattern was used: \\bFROM\\b and was detected 54 times, the first in the element starting with: "\t\t\t\t// Logic borrowed from http://json.org/json2.js\r", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'from', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '172', 'inputVector': '', 'url':

```
'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that
return information that may help an attacker and fix any underlying problems they refer to.', 'alert':
'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure -
Suspicious Comments', 'risk': 'Informational', 'id': '494', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '182', 'inputVector': '', 'url': 'https://
ecampus.psgtech.ac.in/feedback/(S(mltvpupbefxv01gpxzk00x1g))/bootstrap/css/bootstrap.min.css',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '501', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bWHERE\\b and was detected 10 times, the
first in the element starting with: "\t\t\t\t\t\t// Handle the case where IE and Opera return items\r", see
evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'where', 'pluginId':
'10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain
suspicious comments which may help an attacker. Note: Matches made within script blocks or files are
against the entire content not only comments.', 'messageId': '172', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that
return information that may help an attacker and fix any underlying problems they refer to.', 'alert':
'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure -
Suspicious Comments', 'risk': 'Informational', 'id': '502', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '172',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
```

core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '510', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '172', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '520', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '172',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '549', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '172', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit

y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '558', 'alertRef': '10037'}

{'sourceid': '3', 'other': 'CVE-2020-11023\nCVE-2020-11022\nCVE-2015-9251\nCVE-2019-11358\n', 'method': 'GET', 'evidence': 'jquery-1.9.1.js', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library jquery, version 1.9.1 is vulnerable.', 'messageId': '172', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {'CVE-2020-11023': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11023', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2020-11022': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11022', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CVE-2015-9251': 'https://nvd.nist.gov/vuln/detail/CVE-2015-9251', 'CVE-2019-11358': 'https://nvd.nist.gov/vuln/detail/CVE-2019-11358', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/jquery/jquery/issues/2432\nhttp://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/\nhttp://research.insecurelabs.org/jquery/test/\nhttps://blog.jquery.com/2019/04/10/jquery-3-4-0-released/\nhttps://nvd.nist.gov/vuln/detail/CVE-2019-11358\nhttps://github.com/advisories/GHSA-rmxg-73gg-4p98\nhttps://nvd.nist.gov/vuln/detail/CVE-2015-9251\nhttps://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b\nhttps://bugs.jquery.com/ticket/11974\nhttps://github.com/jquery/jquery.com/issues/162\nhttps://blog.jquery.com/2020/04/10/jquery-3-5-0-released/\n', 'solution': 'Please upgrade to the latest version of jquery.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '573', 'alertRef': '10003'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '192', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '577', 'alertRef': '10038-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '193', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/images/templatemo_menu_list_icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati

on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '579', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '192', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '584', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '193', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/images/templatemo_menu_list_icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '586', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL:\n\nhttps://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx\n\nappears to include user input in: \n\na(n) [input] tag [value] attribute \n\nThe user input found was:\nabcd3=Login\n\nThe user-controlled value was:\nlogin', 'method': 'POST', 'evidence': '', 'pluginId': '10031', 'cweid': '20', 'confidence': 'Low', 'wascid': '20', '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.', 'messageId': '190', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A03': 'https://owasp.org/Top10/A03_2021-Injection/', 'CWE-20': 'https://cwe.mitre.org/data/definitions/20.html', 'OWASP_2017_A01': 'https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html', 'solution':

'Validate all input and sanitize output it before writing to any HTML attributes.', 'alert': 'User Controllable HTML Element Attribute (Potential XSS)', 'param': 'abcd3', 'attack': '', 'name': 'User Controllable HTML Element Attribute (Potential XSS)', 'risk': 'Informational', 'id': '589', 'alertRef': '10031'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '192', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '591', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '193', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/images/templatemo_menu_list_icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '592', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '192', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to

suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '597', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '193', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/images/templatemo_menu_list_icon.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '599', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '199', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/arrows.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '604', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '196', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_college_of_technology.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '607', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '199', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/arrows.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '611', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '196', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_college_of_technology.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '613', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '199', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/arrows.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '618', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '199', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/arrows.png', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '623', 'alertRef': '10037'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '196', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_college_of_technology.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '626', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '196', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_college_of_technology.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
```

HTTP Response Header Field(s)', 'risk': 'Low', 'id': '630', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bDEBUG\\b and was detected 13 times, the first in the element starting with: "// Name: MicrosoftAjax.debug.js\r", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'debug', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '203', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKxUvgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriYgReyv3ohx7-ei-o01&t=10c151ff', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '669', 'alertRef': '10027'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bQUERY\\b and was detected in the element starting with: ""historyMissingFrame":"For the history feature to work in IE, the page must have an iFrame element with id \\u0027__historyFrame\\"", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'query', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '203', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKxUvgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriYgReyv3ohx7-ei-o01&t=10c151ff', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '670', 'alertRef': '10027'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bFROM\\b and was detected 2 times, the first in the element starting with: ""invalidExecutorType":"Could not create a valid Sys.Net.WebRequestExecutor from: {0}.",\r", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'from', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '203', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKxUvgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriYgReyv3ohx7-ei-o01&t=10c151ff', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure -

```
Suspicious Comments', 'risk': 'Informational', 'id': '671', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '203',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=nnHyWnZ5bTPu
YszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKxUvgOctjh3nF3Yl4Cco
SALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriYgReyv3ohx7-ei-o01&t
=10c151ff', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '672', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '203', 'inputVector': '', 'url': 'h
ttps://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sd
a5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKxUvgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qx
DJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriYgReyv3ohx7-ei-o01&t=10c151ff', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '673', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method':
'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14',
'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response
header field(s).', 'messageId': '203', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scri
ptResource.axd?d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFE
qmeMCa9PKxUvgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfS
auSm9l3oXsriYgReyv3ohx7-ei-o01&t=10c151ff', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-
project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/
08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933':
'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varun
m/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not
return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name':
'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '674', 'alertRef': '10061'}
```

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '203', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKxUvgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriYgReyv3ohx7-ei-o01&t=10c151ff', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '675', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '203', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKxUvgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriYgReyv3ohx7-ei-o01&t=10c151ff', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '676', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '218', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/engine1/jquery.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This

is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '721', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '210', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '740', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '220', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/psgtechlogo.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '750', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '228', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKxUvgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriYgReyv3ohx7-ei-o01&t=10c151ff', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '782', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '249', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header', 'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id': '852', 'alertRef': '10020-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525', 'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.', 'messageId': '249', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/FbkWfLogin.aspx', 'tags': {'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-recommendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control', 'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '859', 'alertRef': '10015'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '286', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.min.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '862', 'alertRef': '10112'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '251', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '863', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '258', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '865', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '249', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '866', 'alertRef': '10038-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '254', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '867', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '256', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '869', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '257', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '870', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '251', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '871', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an

IETF standards track protocol and is specified in RFC 6797.', 'messageId': '258', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '872', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '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: "__VIEWSTATE" "__VIEWSTATEGENERATOR" "txtpwd" "TxtRollNo"].', 'method': 'GET', 'evidence': '<form method="post" action="./FbkWfLogin.aspx" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '249', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF

Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '873', 'alertRef': '10202'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '256', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '876', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '257', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '877', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '254', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '878', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSER\\b and was detected in the element starting with: "<script type="text/javascript">\r\n\r\n \r\n\r\n $(document).ready(function () {\r\n \r\n \r\n //", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'User', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '249', 'inputVector': '', 'url':

'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '880', 'alertRef': '10027'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '258', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '881', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '251', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':

```
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '882', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '257',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstra
p/css/sweetalert.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '884', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '256',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstra
p/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '885', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '254',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/w3.css', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '886', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '258', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/ecampus.css',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '888', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '251', 'inputVector': '', 'url': 'https://
ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/js/bootstrap.min.js', 'tags':
{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '889', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'No links have been found while there are scripts, which is an indication that this
is a modern web application.', 'method': 'GET', 'evidence': '<script
src="bootstrap/js/jquery-2.1.1.min.js"></script>', 'pluginId': '10109', 'cweid': '-1', 'confidence': 'Medium',
```

'wascid': '-1', '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.', 'messageId': '249', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/FbkWfLogin.aspx', 'tags': {}, 'reference': '', 'solution': 'This is an informational alert and so no changes are required.', 'alert': 'Modern Web Application', 'param': '', 'attack': '', 'name': 'Modern Web Application', 'risk': 'Informational', 'id': '890', 'alertRef': '10109'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '257', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '892', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '256', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '893', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '254', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':

```
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '894', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '249',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '896', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'CVE-2018-14041\nCVE-2019-8331\nCVE-2018-20677\nCVE-2018-20676\nCV
E-2018-14042\nCVE-2016-10735\n', 'method': 'GET', 'evidence': '* Bootstrap v3.3.7', 'pluginId': '10003',
'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library bootstrap, version
3.3.7 is vulnerable.', 'messageId': '251', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S
(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/js/bootstrap.min.js', 'tags': {'CVE-2018-14041':
'https://nvd.nist.gov/vuln/detail/CVE-2018-14041', 'CVE-2019-8331':
'https://nvd.nist.gov/vuln/detail/CVE-2019-8331', 'OWASP_2017_A09': 'https://owasp.org/www-project-t
op-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2018-20677':
'https://nvd.nist.gov/vuln/detail/CVE-2018-20677', 'CVE-2018-20676':
'https://nvd.nist.gov/vuln/detail/CVE-2018-20676', 'CVE-2018-14042':
'https://nvd.nist.gov/vuln/detail/CVE-2018-14042', 'CVE-2016-10735':
'https://nvd.nist.gov/vuln/detail/CVE-2016-10735', 'OWASP_2021_A06':
'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CWE-829':
'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/twbs/bootstrap/issues/2
8236\nhttps://github.com/advisories/GHSA-pj7m-g53m-7638\nhttps://github.com/twbs/bootstrap/issues
/20184\nhttps://github.com/advisories/GHSA-ph58-4vrj-w6hr\nhttps://github.com/twbs/bootstrap/issues/
20631\nhttps://github.com/advisories/GHSA-4p24-vmcr-4gqj\nhttps://github.com/advisories/GHSA-9v3
m-8fp8-mj99\nhttps://nvd.nist.gov/vuln/detail/CVE-2018-20676\n', 'solution': 'Please upgrade to the
latest version of bootstrap.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS
Library', 'risk': 'Medium', 'id': '900', 'alertRef': '10003'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '249', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
```

'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '902', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': 'The following pattern was used: \\bDB\\b and was detected 2 times, the first in the element starting with: "!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.docu", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'db', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '260', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '905', 'alertRef': '10027'}

{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the element starting with: "},removeAttr:function(a,b){var c,d,e=0,f=b&&b.match(E);if(f&&1===a.nodeType)while(c=f[e++])d=n.propFix[c]||c,n.expr.match.bool.t", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'username', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '260', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '911', 'alertRef': '10027'}

{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '249', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/FbkWfLogin.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not

return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '912', 'alertRef': '10061'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=\npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST', 'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.', 'messageId': '242', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request Identified', 'risk': 'Informational', 'id': '914', 'alertRef': '10111'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '261', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '915', 'alertRef': '10036'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '249', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '918', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '260', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '919', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '261', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '920', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '290', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '922', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '249', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',

'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '925', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '260', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '926', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '265', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '929', 'alertRef': '10036'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '261', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05':

'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '930', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '260',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstra
p/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '933', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '261', 'inputVector': '', 'url': 'https://
ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/css/bootstrap.min.css',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '934', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy

mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '265', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '935', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '260', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '941', 'alertRef': '10037'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '265', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '945', 'alertRef': '10021'}

{'sourceid': '3', 'other': 'CVE-2020-11023\nCVE-2020-11022\nCVE-2015-9251\nCVE-2019-11358\n', 'method': 'GET', 'evidence': 'jquery-2.1.1.min.js', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library jquery, version 2.1.1 is vulnerable.', 'messageId': '260', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'CVE-2020-11023': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11023', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2020-11022': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11022', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CVE-2015-9251': 'https://nvd.nist.gov/vuln/detail/CVE-2015-9251', 'CVE-2019-11358': 'https://nvd.nist.gov/vuln/detail/CVE-2019-11358', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/jquery/jquery/issues/2432\nhttp://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/\nhttp://research.insecurelabs.org/jquery/test/\nhttps://blog.jquery.com/2019/04/10/jquery-3-4-0-released/\nhttps://nvd.nist.gov/vuln/detail/CVE-2019-11358\nhttps://github.com/advisories/GHSA-rmxg-73gg-4p98\nhttps://nvd.nist.gov/vuln/detail/CVE-2015-9251\nhttps://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b\nhttps://bugs.jquery.com/ticket/11974\nhttps://github.com/jquery/jquery.com/issues/162\nhttps://blog.jquery.com/2020/04/10/jquery-3-5-0-released/\n', 'solution': 'Please upgrade to the latest version of jquery.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '949', 'alertRef': '10003'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '265', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '952', 'alertRef': '10037'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '294', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/lock.png', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '956', 'alertRef': '10112'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '277', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '984', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '278', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/icon/apple-touch-icon.jpg',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '986', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '278',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/icon/apple-touch-icon.jpg',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '990', 'alertRef': '10036'}
```

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '277', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '992', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '278', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '995', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '277', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '996', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '278', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(r5kaj0bdivvi2b2h5ozqmzmk))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',

'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '1002', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '277', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '1003', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '295', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/modernizr-2.5.3.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '1019', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '297', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '1029', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',

'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '309', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '1051', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '312', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '1076', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '328', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '1173', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '322', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/pause.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '1198', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '322', 'inputVector': '', 'url':

'https://ecampus.psgtech.ac.in/engine1/pause.png', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '1200', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '311', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '1204', 'alertRef': '10112'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '322',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/pause.png', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '1208', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '322', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/engine1/pause.png', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit

y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '1211', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '337', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '1276', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '352', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '1327', 'alertRef': '10112'}
{'sourceid': '3', 'other': '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: "__EVENTARGUMENT" "__EVENTTARGET" "__EVENTVALIDATION" "__LASTFOCUS" "__VIEWSTATE" "__VIEWSTATEGENERATOR" "abcd3" "btnRefresh" "rdolst_0" "rdolst_1" "rdolst_2" "rdolst_3" "txtusercheck"].', 'method': 'POST', 'evidence': '<form method="post" action="./" onsubmit="javascript:return WebForm_OnSubmit();" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '350', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Mana

gement_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05':
'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352':
'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheats
heets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitio
ns/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does
not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor
example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase:
Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF
defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and
Design\nGenerate 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).\nNote that this can be
bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management
control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request
that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF
Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '1347',
'alertRef': '10202'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '396', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '1433', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '384', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?
d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKxU
vgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriYg
Reyv3ohx7-ei-o01&t=10c151ff', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '1436', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '359', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This

is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '1484', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=
\npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST',
'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.', 'messageId': '389', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/',
'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request
Identified', 'risk': 'Informational', 'id': '1620', 'alertRef': '10111'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'POST', 'evidence':
'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '400', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '1633', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '434', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '1654', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '428', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '1708', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=xtIjDAoS
\npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST',
'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.', 'messageId': '423', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request Identified', 'risk': 'Informational', 'id': '1772', 'alertRef': '10111'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '479', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/psgtechlogo.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '1867', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '490', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '1914', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '489', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/modernizr-2.5.3.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '1917', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '503', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '2159', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',

'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '517', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '2222', 'alertRef': '10112'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '506', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/psglogo.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '2223', 'alertRef': '10112'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '513', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header', 'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id': '2233', 'alertRef': '10020-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525', 'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.', 'messageId': '513', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/FbkWfLogin.aspx', 'tags': {'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-recommendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control', 'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '2240', 'alertRef':

'10015'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '513', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '2242', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '525', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '2243', 'alertRef': '10112'}
{'sourceid': '3', 'other': '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: "__VIEWSTATE" "__VIEWSTATEGENERATOR" "txtpwd" "TxtRollNo"].', 'method': 'GET', 'evidence': '<form method="post" action="./FbkWfLogin.aspx" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '513', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/FbkWfLogin.aspx', 'tags':

{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '2246', 'alertRef': '10202'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSER\\b and was detected in the element starting with: "<script type="text/javascript">\r\n\r\n \r\n\r\n $(document).ready(function () {\r\n \r\n \r\n //", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'User', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '513', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '2247', 'alertRef': '10027'}
{'sourceid': '3', 'other': 'No links have been found while there are scripts, which is an indication that this is a modern web application.', 'method': 'GET', 'evidence': '<script src="bootstrap/js/jquery-2.1.1.min.js"></script>', 'pluginId': '10109', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1', '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.', 'messageId': '513', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/FbkWfLogin.aspx', 'tags': {}, 'reference': '', 'solution': 'This is an informational alert and so no changes are required.', 'alert': 'Modern Web Application', 'param': '', 'attack': '', 'name': 'Modern Web Application', 'risk': 'Informational', 'id': '2249', 'alertRef': '10109'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '513',

```
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '2251', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '513', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2253', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method':
'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14',
'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response
header field(s).', 'messageId': '513', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/FbkWfLogin.aspx', 'tags':
{'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933':
'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varun
m/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not
return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name':
'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '2256', 'alertRef': '10061'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '513',
'inputVector': '', 'url':
```

```
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': ", 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2257', 'alertRef': '10021'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '513', 'inputVector': ", 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': ", 'attack': ", 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2258', 'alertRef': '10037'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': ", 'pluginId': '10020', 'cweid': '1021', 'confidence':
'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy
with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.",
'messageId': '515', 'inputVector': ", 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021':
'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project
-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testin
g_for_Clickjacking', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference':
'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern
Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one
of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header',
'param': 'x-frame-options', 'attack': ", 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id':
'2275', 'alertRef': '10020-1'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '521',
'inputVector': ", 'url':
```

'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/sweetalert.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '2278', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '526',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstra
p/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '2279', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '518',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/sweetalert.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '2280', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '524',
'inputVector': '', 'url':

```
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/w3.css', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '2281', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '523',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/bootstrap.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '2282', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '521', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/sweetalert.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2284', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '526', 'inputVector': '', 'url': 'h
ttps://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/js/sweetalert.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2285', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '518', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/sweetalert.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2286', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '524', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/w3.css', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2287', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '523', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/bootstrap.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2288', 'alertRef': '10035-1'}
```

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525',
'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is
missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files
this might be intended, however, the resources should be reviewed to ensure that no sensitive content
will be cached.', 'messageId': '515', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/FbkWfLogin.aspx', 'tags':
{'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/
www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_T
esting/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/
cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla
.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-re
commendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with
"no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives
"public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control',
'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '2289', 'alertRef':
'10015'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '518',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/sweetalert.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2292', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '526',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstra
p/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g

g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2293', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '521', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2294', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '515', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '2296', 'alertRef': '10038-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '523', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2298', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '526', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2299', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '518', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2300', 'alertRef': '10037'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '524', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2301', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '521', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2302', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '523', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We

b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2305', 'alertRef': '10037'}
{'sourceid': '3', 'other': '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: "__VIEWSTATE" "__VIEWSTATEGENERATOR" "txtpwd" "TxtRollNo"].', 'method': 'GET', 'evidence': '<form method="post" action="./FbkWfLogin.aspx" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '515', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '2306', 'alertRef': '10202'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '524', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2307', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '529', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '2308', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '531', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '2309', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '532',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/w3.css', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '2310', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '533',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/ecampus.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '2312', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'CVE-2018-14041\nCVE-2019-8331\nCVE-2018-20677\nCVE-2018-20676\nCV
E-2018-14042\nCVE-2016-10735\n', 'method': 'GET', 'evidence': '* Bootstrap v3.3.7', 'pluginId': '10003',
'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library bootstrap, version
3.3.7 is vulnerable.', 'messageId': '523', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/bootstrap.min.js',
'tags': {'CVE-2018-14041': 'https://nvd.nist.gov/vuln/detail/CVE-2018-14041', 'CVE-2019-8331':
'https://nvd.nist.gov/vuln/detail/CVE-2019-8331', 'OWASP_2017_A09': 'https://owasp.org/www-project-t
op-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2018-20677':
'https://nvd.nist.gov/vuln/detail/CVE-2018-20677', 'CVE-2018-20676':
'https://nvd.nist.gov/vuln/detail/CVE-2018-20676', 'CVE-2018-14042':
'https://nvd.nist.gov/vuln/detail/CVE-2018-14042', 'CVE-2016-10735':
'https://nvd.nist.gov/vuln/detail/CVE-2016-10735', 'OWASP_2021_A06':
'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CWE-829':
'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/twbs/bootstrap/issues/2
8236\nhttps://github.com/advisories/GHSA-pj7m-g53m-7638\nhttps://github.com/twbs/bootstrap/issues
/20184\nhttps://github.com/advisories/GHSA-ph58-4vrj-w6hr\nhttps://github.com/twbs/bootstrap/issues/
20631\nhttps://github.com/advisories/GHSA-4p24-vmcr-4gqj\nhttps://github.com/advisories/GHSA-9v3
m-8fp8-mj99\nhttps://nvd.nist.gov/vuln/detail/CVE-2018-20676\n', 'solution': 'Please upgrade to the
latest version of bootstrap.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS
Library', 'risk': 'Medium', 'id': '2313', 'alertRef': '10003'}
```

{'sourceid': '3', 'other': 'The following pattern was used: \\bUSER\\b and was detected in the element starting with: "<script type="text/javascript">\r\n\r\n \r\n\r\n $(document).ready(function () {\r\n \r\n \r\n //", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'User', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '515', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '2314', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '529', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2315', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '531', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2316', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '532', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':

'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2317', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '533', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2319', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '535', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '2320', 'alertRef': '10036'}

{'sourceid': '3', 'other': 'No links have been found while there are scripts, which is an indication that this is a modern web application.', 'method': 'GET', 'evidence': '<script src="bootstrap/js/jquery-2.1.1.min.js"></script>', 'pluginId': '10109', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1', '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.', 'messageId': '515', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/FbkWfLogin.aspx', 'tags': {}, 'reference': '', 'solution': 'This is an informational alert and so no changes are required.', 'alert': 'Modern Web Application', 'param': '', 'attack': '', 'name': 'Modern Web Application', 'risk': 'Informational', 'id': '2321', 'alertRef': '10109'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '531',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/js/bootstrap.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2322', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '529',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/sweetalert.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2323', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '532',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/w3.css', 'tags':

{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2325', 'alertRef': '10021'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bDB\\b and was detected 2 times, the first in the element starting with: "!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.docu", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'db', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '534', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '2326', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '535', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2327', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '533', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/ecampus.css',

'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2328', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '515', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '2329', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '529', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2330', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '531', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/js/bootstrap.min.js',

'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2331', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the element starting with: "},removeAttr:function(a,b){var c,d,e=0,f=b&&b.match(E);if(f&&1===a.nodeType)while(c=f[e++])d=n.propFix[c]||c,n.expr.match.bool.t", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'username', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '534', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '2333', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '532', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2334', 'alertRef': '10037'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '535', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2335', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '533', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2336', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '515', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2337', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '534',

'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '2339', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '535', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2341', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'CVE-2018-14041\nCVE-2019-8331\nCVE-2018-20677\nCVE-2018-20676\nCVE-2018-14042\nCVE-2016-10735\n', 'method': 'GET', 'evidence': '* Bootstrap v3.3.7', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library bootstrap, version 3.3.7 is vulnerable.', 'messageId': '531', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/js/bootstrap.min.js', 'tags': {'CVE-2018-14041': 'https://nvd.nist.gov/vuln/detail/CVE-2018-14041', 'CVE-2019-8331': 'https://nvd.nist.gov/vuln/detail/CVE-2019-8331', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2018-20677': 'https://nvd.nist.gov/vuln/detail/CVE-2018-20677', 'CVE-2018-20676': 'https://nvd.nist.gov/vuln/detail/CVE-2018-20676', 'CVE-2018-14042': 'https://nvd.nist.gov/vuln/detail/CVE-2018-14042', 'CVE-2016-10735': 'https://nvd.nist.gov/vuln/detail/CVE-2016-10735', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/twbs/bootstrap/issues/28236\nhttps://github.com/advisories/GHSA-pj7m-g53m-7638\nhttps://github.com/twbs/bootstrap/issues/20184\nhttps://github.com/advisories/GHSA-ph58-4vrj-w6hr\nhttps://github.com/twbs/bootstrap/issues/20631\nhttps://github.com/advisories/GHSA-4p24-vmcr-4gqj\nhttps://github.com/advisories/GHSA-9v3m-8fp8-mj99\nhttps://nvd.nist.gov/vuln/detail/CVE-2018-20676\n', 'solution': 'Please upgrade to the latest version of bootstrap.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '2342', 'alertRef': '10003'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14',

'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '515', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/FbkWfLogin.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '2343', 'alertRef': '10061'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bDB\\b and was detected 2 times, the first in the element starting with: "!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.docu", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'db', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '536', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '2344', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '534', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2345', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'POST', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '573', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session

Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '2347', 'alertRef': '10112'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '515', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2348', 'alertRef': '10021'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the element starting with: "},removeAttr:function(a,b){var c,d,e=0,f=b&&b.match(E);if(f&&1===a.nodeType)while(c=f[e++])d=n.propFix[c]||c,n.expr.match.bool.t", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'username', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '536', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '2350', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '541', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/

core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '2352', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '515', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2353', 'alertRef': '10037'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '534', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2355', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '536', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',

'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '2356', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '538', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '2358', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '541', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2360', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '534', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':

'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2362', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '536', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2365', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '538', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2366', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '541', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g

g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': ", 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2368', 'alertRef': '10021'}
{'sourceid': '3', 'other': 'CVE-2020-11023\nCVE-2020-11022\nCVE-2015-9251\nCVE-2019-11358\n',
'method': 'GET', 'evidence': 'jquery-2.1.1.min.js', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium',
'wascid': '-1', 'description': 'The identified library jquery, version 2.1.1 is vulnerable.', 'messageId': '534',
'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstra
p/js/jquery-2.1.1.min.js', 'tags': {'CVE-2020-11023': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11023',
'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_
Known_Vulnerabilities.html', 'CVE-2020-11022': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11022',
'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/',
'CVE-2015-9251': 'https://nvd.nist.gov/vuln/detail/CVE-2015-9251', 'CVE-2019-11358':
'https://nvd.nist.gov/vuln/detail/CVE-2019-11358', 'CWE-829':
'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/jquery/jquery/issues/24
32\nhttp://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/\nhttp://research.insecurelabs.org/
jquery/test/\nhttps://blog.jquery.com/2019/04/10/jquery-3-4-0-released/\nhttps://nvd.nist.gov/vuln/detail/
CVE-2019-11358\nhttps://github.com/advisories/GHSA-rmxg-73gg-4p98\nhttps://nvd.nist.gov/vuln/deta
il/CVE-2015-9251\nhttps://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd08086
19b1b\nhttps://bugs.jquery.com/ticket/11974\nhttps://github.com/jquery/jquery.com/issues/162\nhttps://
blog.jquery.com/2020/04/10/jquery-3-5-0-released/\n', 'solution': 'Please upgrade to the latest version of
jquery.', 'alert': 'Vulnerable JS Library', 'param': ", 'attack': ", 'name': 'Vulnerable JS Library', 'risk':
'Medium', 'id': '2371', 'alertRef': '10003'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '541', 'inputVector': ", 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/Images/psg_tech.jpg', 'tags':
{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': ", 'attack': ", 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2373', 'alertRef': '10037'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': ", 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '545', 'inputVector': ", 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/icon/apple-touch-icon.jpg', 'tags':

{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '2374', 'alertRef': '10038-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '536', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2379', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '545', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '2380', 'alertRef': '10036'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server

error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '538', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2386', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '536', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2387', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '545', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2388', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '538', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2393', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '576', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '2394', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'CVE-2020-11023\nCVE-2020-11022\nCVE-2015-9251\nCVE-2019-11358\n', 'method': 'GET', 'evidence': 'jquery-2.1.1.min.js', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library jquery, version 2.1.1 is vulnerable.', 'messageId': '536', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'CVE-2020-11023': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11023', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2020-11022': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11022', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CVE-2015-9251': 'https://nvd.nist.gov/vuln/detail/CVE-2015-9251', 'CVE-2019-11358': 'https://nvd.nist.gov/vuln/detail/CVE-2019-11358', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/jquery/jquery/issues/2432\nhttp://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/\nhttp://research.insecurelabs.org/jquery/test/\nhttps://blog.jquery.com/2019/04/10/jquery-3-4-0-released/\nhttps://nvd.nist.gov/vuln/detail/CVE-2019-11358\nhttps://github.com/advisories/GHSA-rmxg-73gg-4p98\nhttps://nvd.nist.gov/vuln/detail/CVE-2015-9251\nhttps://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b\nhttps://bugs.jquery.com/ticket/11974\nhttps://github.com/jquery/jquery.com/issues/162\nhttps://blog.jquery.com/2020/04/10/jquery-3-5-0-released/\n', 'solution': 'Please upgrade to the latest version of jquery.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '2395', 'alertRef': '10003'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '545', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(icnsh50v23elrcanfblszi4i))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2396', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '552', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '2400', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '550', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '2401', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '549', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '2406', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '552', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '2407', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '550', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2408', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to

interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '549', 'inputVector': '', 'url': 'h
ttps://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/bootstrap.min.cs
s', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2412', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '552', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/icon/apple-touch-icon.jpg',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '2415', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '550',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/Images/psg_tech.jpg', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2418', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '552', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/icon/apple-touch-icon.jpg',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2420', 'alertRef': '10037'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '549',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstra
p/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '2425', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '550', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/Images/psg_tech.jpg', 'tags':
{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
```

HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2426', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '549', 'inputVector': '', 'url': 'https://
ecampus.psgtech.ac.in/feedback/(S(52jksw1n3ve2wit2dtziebm1))/bootstrap/css/bootstrap.min.css',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '2430', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '584', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/psglogo.jpg', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '2547', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'POST', 'evidence':
'3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '601', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '2635', 'alertRef': '10112'}
{'sourceid': '3', 'other': '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:
"__EVENTARGUMENT" "__EVENTTARGET" "__EVENTVALIDATION" "__LASTFOCUS"
"__VIEWSTATE" "__VIEWSTATEGENERATOR" "abcd3" "btnRefresh" "rdolst_0" "rdolst_1" "rdolst_2"
"rdolst_3" "txtpwdcheck" "txtusercheck"].', 'method': 'POST', 'evidence': '<form method="post"
action="Attwfloginpage.aspx" onsubmit="javascript:return WebForm_OnSubmit();" id="form1">',
'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens
were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing
a victim to send an HTTP request to a target destination without their knowledge or intent in order to
perform an action as the victim. The underlying cause is application functionality using predictable
URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a

```
web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a
web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request
forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea
surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active
session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The
victim is on the same local network as the target site.\n\nCSRF 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.",
'messageId': '613', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags':
{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery',
'OWASP_2017_A05':
'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352':
'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheats
heets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitio
ns/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does
not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor
example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase:
Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF
defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and
Design\nGenerate 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).\nNote that this can be
bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management
control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request
that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF
Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '2745',
'alertRef': '10202'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '624', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Images/psgtechlogo.jpg', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '2746', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=LOvizMRu
\npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST',
'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.', 'messageId': '608', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/',
'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request
Identified', 'risk': 'Informational', 'id': '2751', 'alertRef': '10111'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '612', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '2784', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '627', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '2837', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '651', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?
d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKxU
vgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriYg
Reyv3ohx7-ei-o01&t=10c151ff', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '2883', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'POST', 'evidence':
'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '658', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '2943', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1',
```

'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '648', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '2974', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '665', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3005', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '666', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3011', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '696', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3033', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '679', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?
d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKxU
vgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriYg
Reyv3ohx7-ei-o01&t=10c151ff', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This

is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3047', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '698', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.min.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3098', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '699', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3128', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '702', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/_references.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3157', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '703', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/psglogo.jpg', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3164', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session

Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '705', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '3177', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '735', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/modernizr-2.5.3.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '3350', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '712', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '3356', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '737', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/_references.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '3359', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '743', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/css/responsive.css', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This

is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '3417', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=bUkCMvnK \npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST', 'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.', 'messageId': '719', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request Identified', 'risk': 'Informational', 'id': '3423', 'alertRef': '10111'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'POST', 'evidence': 'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '744', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '3429', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '747', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '3447', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '750', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.min.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '3464', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session

Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '764', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3616', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cbhqk1udfl33y2lkmebsut4i', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '765', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3630', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '776', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg',
'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3689', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cbhqk1udfl33y2lkmebsut4i', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '799', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3692', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '801', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3750', 'alertRef': '10112'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '792', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/psglogo.jpg', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3774', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=WQWsJZhw
\npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST',
'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.', 'messageId': '787', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/',
'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request
Identified', 'risk': 'Informational', 'id': '3804', 'alertRef': '10111'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '802', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3819', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '839', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.min.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3877', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '838', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/play.png', 'tags': {},

'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3878', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '843', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert-dev.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3903', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '846', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3931', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '844', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3935', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '824', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg',
'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '3940', 'alertRef': '10112'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '848', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert-dev.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '3960', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '819', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '3967', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '850', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/modernizr-2.5.3.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '3988', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '852', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4007', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to

"Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '851', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/modernizr-2.5.3.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4013', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '838', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/play.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4019', 'alertRef': '10036'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '856', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/lock.png', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4022', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '838', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/play.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4024', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server

error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '838', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/play.png', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4029', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '838', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/play.png', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4030', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '858', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/lock.png', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4031', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.',

'messageId': '860', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4045', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '859', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4061', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '853', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/play.png', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4148', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '901', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/bootstrap.min.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4190', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '873', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(wtl5xjhuettwaie3mebdyu2n))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand

p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4201', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '873', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(wtl5xjhuettwaie3mebdyu2n))/FbkWfLogin.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '4203', 'alertRef': '10061'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '873', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(wtl5xjhuettwaie3mebdyu2n))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4205', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '876', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header',

'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id':
'4210', 'alertRef': '10020-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525',
'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is
missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files
this might be intended, however, the resources should be reviewed to ensure that no sensitive content
will be cached.', 'messageId': '876', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/FbkWfLogin.aspx', 'tags':
{'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/
www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_T
esting/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/
cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla
.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-re
commendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with
"no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives
"public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control',
'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '4217', 'alertRef':
'10015'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '876', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '4221', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '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:
"__VIEWSTATE" "__VIEWSTATEGENERATOR" "txtpwd" "TxtRollNo"].', 'method': 'GET', 'evidence':
'<form method="post" action="./FbkWfLogin.aspx" id="form1">', 'pluginId': '10202', 'cweid': '352',
'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission
form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request
to a target destination without their knowledge or intent in order to perform an action as the victim. The
underlying cause is application functionality using predictable URL/form actions in a repeatable way.
The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast,
cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are
not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF,
one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a
number of situations, including:\n * The victim has an active session on the target site.\n * The victim is
authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target
site.\n\nCSRF 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.", 'messageId': '876', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '4225', 'alertRef': '10202'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '903', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/psglogo.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4227', 'alertRef': '10112'}

{'sourceid': '3', 'other': 'The following pattern was used: \\bUSER\\b and was detected in the element starting with: "<script type="text/javascript">\r\n\r\n \r\n\r\n $(document).ready(function () {\r\n \r\n \r\n //", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'User', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '876', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert':

'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '4231', 'alertRef': '10027'}
{'sourceid': '3', 'other': 'No links have been found while there are scripts, which is an indication that this is a modern web application.', 'method': 'GET', 'evidence': '<script src="bootstrap/js/jquery-2.1.1.min.js"></script>', 'pluginId': '10109', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1', '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.', 'messageId': '876', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/FbkWfLogin.aspx', 'tags': {}, 'reference': '', 'solution': 'This is an informational alert and so no changes are required.', 'alert': 'Modern Web Application', 'param': '', 'attack': '', 'name': 'Modern Web Application', 'risk': 'Informational', 'id': '4238', 'alertRef': '10109'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'cbhqk1udfl33y2lkmebsut4i', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '915', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/modernizr-2.5.3.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4243', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '876', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4248', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '876', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo

rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4253', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '897', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Images/psgtechlogo.jpg', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '4261', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method':
'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14',
'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response
header field(s).', 'messageId': '876', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/FbkWfLogin.aspx', 'tags':
{'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varun
m/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not
return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name':
'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '4262', 'alertRef': '10061'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '876',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4269', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '876', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4273', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '919', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/icon', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4280', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '889', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4301', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '889', 'inputVector': '', 'url':

'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4303', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '889', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4307', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '889', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4311', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'cbhqk1udfl33y2lkmebsut4i', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The

\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '929', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/images/psg-logo.png', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4320', 'alertRef': '10112'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '896', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4324', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '892', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4325', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '894', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':

'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4327', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '896', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4331', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '892', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4332', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '894', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce

Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4337', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '896',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/ecampus.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4339', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '892',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/sweetalert.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4340', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '894', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4345', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '892', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4346', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '896', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4347', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '894', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4348', 'alertRef': '10037'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'cbhqk1udfl33y2lkmebsut4i', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '934', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4350', 'alertRef': '10112'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '901', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4360', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '901', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':

'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4375', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '943', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/modernizr-2.5.3.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4377', 'alertRef': '10112'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '901', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4379', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '901', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit

y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4385', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'CVE-2018-14041\nCVE-2019-8331\nCVE-2018-20677\nCVE-2018-20676\nCVE-2018-14042\nCVE-2016-10735\n', 'method': 'GET', 'evidence': '* Bootstrap v3.3.7', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library bootstrap, version 3.3.7 is vulnerable.', 'messageId': '901', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/bootstrap.min.js', 'tags': {'CVE-2018-14041': 'https://nvd.nist.gov/vuln/detail/CVE-2018-14041', 'CVE-2019-8331': 'https://nvd.nist.gov/vuln/detail/CVE-2019-8331', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2018-20677': 'https://nvd.nist.gov/vuln/detail/CVE-2018-20677', 'CVE-2018-20676': 'https://nvd.nist.gov/vuln/detail/CVE-2018-20676', 'CVE-2018-14042': 'https://nvd.nist.gov/vuln/detail/CVE-2018-14042', 'CVE-2016-10735': 'https://nvd.nist.gov/vuln/detail/CVE-2016-10735', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/twbs/bootstrap/issues/28236\nhttps://github.com/advisories/GHSA-pj7m-g53m-7638\nhttps://github.com/twbs/bootstrap/issues/20184\nhttps://github.com/advisories/GHSA-ph58-4vrj-w6hr\nhttps://github.com/twbs/bootstrap/issues/20631\nhttps://github.com/advisories/GHSA-4p24-vmcr-4gqj\nhttps://github.com/advisories/GHSA-9v3m-8fp8-mj99\nhttps://nvd.nist.gov/vuln/detail/CVE-2018-20676\n', 'solution': 'Please upgrade to the latest version of bootstrap.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '4398', 'alertRef': '10003'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bDB\\b and was detected 2 times, the first in the element starting with: "!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.docu", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'db', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '905', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '4402', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '908', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/

core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4403', 'alertRef': '10036'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '940', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4404', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the element starting with: "},removeAttr:function(a,b){var c,d,e=0,f=b&&b.match(E);if(f&&1===a.nodeType)while(c=f[e++])d=n.propFix[c]||c,n.expr.match.bool.t", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'username', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '905', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '4408', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '908', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4409', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '912',

```
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/Images/psg_tech.jpg', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '4412', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '905',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/
js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '4416', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '912', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/Images/psg_tech.jpg', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4419', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '905', 'inputVector': '', 'url': 'h
ttps://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/jquery-2.1.1.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4423', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '908',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/
css/bootstrap.min.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4424', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '912',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/Images/psg_tech.jpg', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4427', 'alertRef': '10021'}
```

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '908', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4429', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '916', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '4431', 'alertRef': '10038-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '905', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the

application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4432', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '912', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4433', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '916', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4435', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '905', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':

'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4436', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '916', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4442', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'CVE-2020-11023\nCVE-2020-11022\nCVE-2015-9251\nCVE-2019-11358\n', 'method': 'GET', 'evidence': 'jquery-2.1.1.min.js', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library jquery, version 2.1.1 is vulnerable.', 'messageId': '905', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'CVE-2020-11023': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11023', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2020-11022': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11022', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CVE-2015-9251': 'https://nvd.nist.gov/vuln/detail/CVE-2015-9251', 'CVE-2019-11358': 'https://nvd.nist.gov/vuln/detail/CVE-2019-11358', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/jquery/jquery/issues/2432\nhttp://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/\nhttp://research.insecurelabs.org/jquery/test/\nhttps://blog.jquery.com/2019/04/10/jquery-3-4-0-released/\nhttps://nvd.nist.gov/vuln/detail/CVE-2019-11358\nhttps://github.com/advisories/GHSA-rmxg-73gg-4p98\nhttps://nvd.nist.gov/vuln/detail/CVE-2015-9251\nhttps://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b\nhttps://bugs.jquery.com/ticket/11974\nhttps://github.com/jquery/jquery.com/issues/162\nhttps://blog.jquery.com/2020/04/10/jquery-3-5-0-released/\n', 'solution': 'Please upgrade to the latest version of jquery.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '4444', 'alertRef': '10003'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '916', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(pl1gkw5fusjzbhtc5q1w5cjn))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit

y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4448', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '956', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4556', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '950', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/psgtechlogo.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4595', 'alertRef': '10112'}
{'sourceid': '3', 'other': '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: "__EVENTARGUMENT" "__EVENTTARGET" "__EVENTVALIDATION" "__LASTFOCUS" "__VIEWSTATE" "__VIEWSTATEGENERATOR" "abcd3" "btnRefresh" "rdolst_0" "rdolst_1" "rdolst_2" "rdolst_3" "txtusercheck"].', 'method': 'POST', 'evidence': '<form method="post" action="./AttWfLoginPage.aspx" onsubmit="javascript:return WebForm_OnSubmit();" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '955', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {'OWASP_2021_A01':

'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '4643', 'alertRef': '10202'}

{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=\npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'method': 'POST', 'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', '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.', 'messageId': '955', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request Identified', 'risk': 'Informational', 'id': '4672', 'alertRef': '10111'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'POST', 'evidence': 'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '955', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4675', 'alertRef': '10112'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1006', 'inputVector': '', 'url':

```
'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.min.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '4708', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '969',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(c2qchruicc0gjm1wakpr2upp))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '4722', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '972',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(l4a51isbjbq1a4u2dxiru3sj))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '4725', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method':
'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14',
'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response
header field(s).', 'messageId': '969', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(c2qchruicc0gjm1wakpr2upp))/FbkWfLogin.aspx', 'tags':
{'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933':
'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varun
m/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not
```

return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '4729', 'alertRef': '10061'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '972', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(l4a51isbjbq1a4u2dxiru3sj))/FbkWfLogin.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '4732', 'alertRef': '10061'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1005', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/bootstrap.min.css', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4733', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '969', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(c2qchruicc0gjm1wakpr2upp))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4737', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '972', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(l4a51isbjbq1a4u2dxiru3sj))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',

'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4739', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '975', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(ajshgqyl3mm01z4rabhwgbq1))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4743', 'alertRef': '10036'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1011', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/Images', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4748', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '975', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(ajshgqyl3mm01z4rabhwgbq1))/FbkWfLogin.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not

return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '4754', 'alertRef': '10061'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '978', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header', 'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id': '4758', 'alertRef': '10020-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '975', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(ajshgqyl3mm01z4rabhwgbq1))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4761', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525', 'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.', 'messageId': '978', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/FbkWfLogin.aspx', 'tags': {'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-recommendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control', 'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '4768', 'alertRef':

'10015'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1016', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/icon', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '4770', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '978', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '4775', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '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:
"__VIEWSTATE" "__VIEWSTATEGENERATOR" "txtpwd" "TxtRollNo"].', 'method': 'GET', 'evidence':
'<form method="post" action="./FbkWfLogin.aspx" id="form1">', 'pluginId': '10202', 'cweid': '352',
'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission
form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request
to a target destination without their knowledge or intent in order to perform an action as the victim. The
underlying cause is application functionality using predictable URL/form actions in a repeatable way.
The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast,
cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are
not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF,
one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a
number of situations, including:\n * The victim has an active session on the target site.\n * The victim is
authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target
site.\n\nCSRF 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.", 'messageId': '978', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/FbkWfLogin.aspx', 'tags':

{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '4781', 'alertRef': '10202'}

{'sourceid': '3', 'other': 'The following pattern was used: \\bUSER\\b and was detected in the element starting with: "<script type="text/javascript">\r\n\r\n \r\n\r\n $(document).ready(function () {\r\n \r\n \r\n //", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'User', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '978', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '4794', 'alertRef': '10027'}

{'sourceid': '3', 'other': 'No links have been found while there are scripts, which is an indication that this is a modern web application.', 'method': 'GET', 'evidence': '<script src="bootstrap/js/jquery-2.1.1.min.js"></script>', 'pluginId': '10109', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1', '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.', 'messageId': '978', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/FbkWfLogin.aspx', 'tags': {}, 'reference': '', 'solution': 'This is an informational alert and so no changes are required.', 'alert': 'Modern Web Application', 'param': '', 'attack': '', 'name': 'Modern Web Application', 'risk': 'Informational', 'id': '4797', 'alertRef': '10109'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '978',

'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4804', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '978', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4811', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '978', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/FbkWfLogin.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '4820', 'alertRef': '10061'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '978', 'inputVector': '', 'url':

'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4827', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '978', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4837', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '991', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4850', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '991', 'inputVector': '', 'url':

'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4856', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '996', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4858', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '996', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4862', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '991', 'inputVector': '', 'url':

'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4865', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '991', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4869', 'alertRef': '10037'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '996', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4870', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1000', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4873', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '996', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4876', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1000', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4877', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1003', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4881', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1002', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4882', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1003', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4883', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1000',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap
/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4886', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1002', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/js/bootstrap.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4887', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1000', 'inputVector': '', 'url': 'https:
//ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/js/sweetalert.min.js',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4889', 'alertRef': '10037'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
```

error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1003', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4890', 'alertRef': '10021'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bDB\\b and was detected 2 times, the first in the element starting with: "!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.docu", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'db', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1004', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '4892', 'alertRef': '10027'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1002', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4893', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1005',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap
/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '4894', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1003', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/ecampus.css',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4895', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the
element starting with: "},removeAttr:function(a,b){var
c,d,e=0,f=b&&b.match(E);if(f&&1===a.nodeType)while(c=f[e++])d=n.propFix[c]||c,n.expr.match.bool.t",
see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'username',
'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears
to contain suspicious comments which may help an attacker. Note: Matches made within script blocks
or files are against the entire content not only comments.', 'messageId': '1004', 'inputVector': '', 'url': 'htt
ps://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/js/jquery-2.1.1.min.js',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leaka
ge', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that

return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '4897', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1005', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4899', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1002', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4900', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1004', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4903', 'alertRef': '10036'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1005', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4904', 'alertRef': '10021'}

{'sourceid': '3', 'other': 'CVE-2018-14041\nCVE-2019-8331\nCVE-2018-20677\nCVE-2018-20676\nCVE-2018-14042\nCVE-2016-10735\n', 'method': 'GET', 'evidence': '* Bootstrap v3.3.7', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library bootstrap, version 3.3.7 is vulnerable.', 'messageId': '1002', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/js/bootstrap.min.js', 'tags': {'CVE-2018-14041': 'https://nvd.nist.gov/vuln/detail/CVE-2018-14041', 'CVE-2019-8331': 'https://nvd.nist.gov/vuln/detail/CVE-2019-8331', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2018-20677': 'https://nvd.nist.gov/vuln/detail/CVE-2018-20677', 'CVE-2018-20676': 'https://nvd.nist.gov/vuln/detail/CVE-2018-20676', 'CVE-2018-14042': 'https://nvd.nist.gov/vuln/detail/CVE-2018-14042', 'CVE-2016-10735': 'https://nvd.nist.gov/vuln/detail/CVE-2016-10735', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/twbs/bootstrap/issues/28236\nhttps://github.com/advisories/GHSA-pj7m-g53m-7638\nhttps://github.com/twbs/bootstrap/issues/20184\nhttps://github.com/advisories/GHSA-ph58-4vrj-w6hr\nhttps://github.com/twbs/bootstrap/issues/20631\nhttps://github.com/advisories/GHSA-4p24-vmcr-4gqj\nhttps://github.com/advisories/GHSA-9v3m-8fp8-mj99\nhttps://nvd.nist.gov/vuln/detail/CVE-2018-20676\n', 'solution': 'Please upgrade to the latest version of bootstrap.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '4905', 'alertRef': '10003'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1004', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo

rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4907', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1005', 'inputVector': '', 'url': 'https:
//ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/css/bootstrap.min.css',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4911', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue= \npasswordParam=txtpwdcheck\nreferer
=https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'method': 'POST', 'evidence':
'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', '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.', 'messageId': '999', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/', 'solution': 'This is an
informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Authentication
Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request Identified', 'risk':
'Informational', 'id': '4912', 'alertRef': '10111'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '1004',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap
/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4913', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1004', 'inputVector': '', 'url': 'https:
//ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap/js/jquery-2.1.1.min.js',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4915', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'CVE-2020-11023\nCVE-2020-11022\nCVE-2015-9251\nCVE-2019-11358\n',
'method': 'GET', 'evidence': 'jquery-2.1.1.min.js', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium',
'wascid': '-1', 'description': 'The identified library jquery, version 2.1.1 is vulnerable.', 'messageId': '1004',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/bootstrap
/js/jquery-2.1.1.min.js', 'tags': {'CVE-2020-11023': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11023',
'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_
Known_Vulnerabilities.html', 'CVE-2020-11022': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11022',
'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/',
'CVE-2015-9251': 'https://nvd.nist.gov/vuln/detail/CVE-2015-9251', 'CVE-2019-11358':
'https://nvd.nist.gov/vuln/detail/CVE-2019-11358', 'CWE-829':
'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/jquery/jquery/issues/24
32\nhttp://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/\nhttp://research.insecurelabs.org/
jquery/test/\nhttps://blog.jquery.com/2019/04/10/jquery-3-4-0-released/\nhttps://nvd.nist.gov/vuln/detail/
CVE-2019-11358\nhttps://github.com/advisories/GHSA-rmxg-73gg-4p98\nhttps://nvd.nist.gov/vuln/deta
il/CVE-2015-9251\nhttps://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd08086
19b1b\nhttps://bugs.jquery.com/ticket/11974\nhttps://github.com/jquery/jquery.com/issues/162\nhttps://
blog.jquery.com/2020/04/10/jquery-3-5-0-released/\n', 'solution': 'Please upgrade to the latest version of
jquery.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk':
'Medium', 'id': '4917', 'alertRef': '10003'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1024', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '4918', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '1013', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '4920', 'alertRef': '10038-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1007', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4922', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1007', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4930', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1013', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '4934', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1013', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '4938', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1007', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '4942', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1007', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4943', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1013', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(jqdkrbg0c3sgx54lphuv2bev))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '4945', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'cbhqk1udfl33y2lkmebsut4i', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1023', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '4980', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=GHMkfuYfwfeBmekr\npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST', 'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.', 'messageId': '1027', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/',
'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request
Identified', 'risk': 'Informational', 'id': '5022', 'alertRef': '10111'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cbhqk1udfl33y2lkmebsut4i', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1032', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/play.png', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '5060', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1037', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '5074', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1046',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstr
ap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '5077', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1049',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/css/w3.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
```

'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '5081', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1046', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '5082', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '1043', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header', 'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id': '5084', 'alertRef': '10020-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1049', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt

ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '5086', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '1046',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstr
ap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '5087', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525',
'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is
missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files
this might be intended, however, the resources should be reviewed to ensure that no sensitive content
will be cached.', 'messageId': '1043', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/FbkWfLogin.aspx', 'tags':
{'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/
www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_T
esting/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/
cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla
.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-re
commendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with
"no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives
"public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control',
'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '5088', 'alertRef':
'10015'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1051',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstr
ap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati

on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '5090', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1052', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '5092', 'alertRef': '10036'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1049', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '5093', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1046', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/js/sweetalert.min.js',

'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '5094', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cbhqk1udfl33y2lkmebsut4i', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1069', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/icon', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '5095', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '1043', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '5096', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1049', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/css/w3.css',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':

'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '5099', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1051', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '5100', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '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: "__VIEWSTATE" "__VIEWSTATEGENERATOR" "txtpwd" "TxtRollNo"].', 'method': 'GET', 'evidence': '<form method="post" action="./FbkWfLogin.aspx" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '1043', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor

example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '5101', 'alertRef': '10202'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1052', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '5102', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSER\\b and was detected in the element starting with: "<script type="text/javascript">\r\n\r\n \r\n\r\n $(document).ready(function () {\r\n \r\n \r\n //", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'User', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1043', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '5109', 'alertRef': '10027'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1052',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstr
ap/css/sweetalert.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '5112', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '1051',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstr
ap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '5115', 'alertRef': '10021'}
{'sourceid': '3', 'other': 'No links have been found while there are scripts, which is an indication that this
is a modern web application.', 'method': 'GET', 'evidence': '<script
src="bootstrap/js/jquery-2.1.1.min.js"></script>', 'pluginId': '10109', 'cweid': '-1', 'confidence': 'Medium',
'wascid': '-1', '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.',
'messageId': '1043', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/FbkWfLogin.aspx', 'tags': {},
'reference': '', 'solution': 'This is an informational alert and so no changes are required.', 'alert': 'Modern
Web Application', 'param': '', 'attack': '', 'name': 'Modern Web Application', 'risk': 'Informational', 'id':
'5117', 'alertRef': '10109'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1052', 'inputVector': '', 'url': 'https:
//ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/css/sweetalert.css',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',

'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '5121', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1051', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '5124', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1043', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '5126', 'alertRef': '10036'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'cbhqk1udfl33y2lkmebsut4i', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.',

'messageId': '1080', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/Images', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '5131', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1043', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '5132', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '1043', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/FbkWfLogin.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '5144', 'alertRef': '10061'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'POST', 'evidence': 'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1076', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '5145', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1058', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':

'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '5147', 'alertRef': '10036'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1043', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '5150', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1058', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '5154', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1043', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/FbkWfLogin.aspx', 'tags':

{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '5157', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1059', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '5158', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=mdFiWApp \npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST', 'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.', 'messageId': '1042', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request Identified', 'risk': 'Informational', 'id': '5159', 'alertRef': '10111'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1058', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':

'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '5162', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1059', 'inputVector': '', 'url': '
https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/js/bootstrap.min.j
s', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '5165', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1058', 'inputVector': '', 'url': 'https:
//ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/css/ecampus.css',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '5167', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1057', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg',
'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session

Management Response Identified', 'risk': 'Informational', 'id': '5171', 'alertRef': '10112'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1059', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '5172', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '1066', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '5178', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1059', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':

'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '5179', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bDB\\b and was detected 2 times, the first in the element starting with: "!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.docu", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'db', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1060', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '5180', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1066', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '5185', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the element starting with: "},removeAttr:function(a,b){var c,d,e=0,f=b&&b.match(E);if(f&&1===a.nodeType)while(c=f[e++])d=n.propFix[c]||c,n.expr.match.bool.t", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'username', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1060', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leaka

ge', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '5186', 'alertRef': '10027'}

{'sourceid': '3', 'other': 'CVE-2018-14041\nCVE-2019-8331\nCVE-2018-20677\nCVE-2018-20676\nCVE-2018-14042\nCVE-2016-10735\n', 'method': 'GET', 'evidence': '* Bootstrap v3.3.7', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library bootstrap, version 3.3.7 is vulnerable.', 'messageId': '1059', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/js/bootstrap.min.js', 'tags': {'CVE-2018-14041': 'https://nvd.nist.gov/vuln/detail/CVE-2018-14041', 'CVE-2019-8331': 'https://nvd.nist.gov/vuln/detail/CVE-2019-8331', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2018-20677': 'https://nvd.nist.gov/vuln/detail/CVE-2018-20677', 'CVE-2018-20676': 'https://nvd.nist.gov/vuln/detail/CVE-2018-20676', 'CVE-2018-14042': 'https://nvd.nist.gov/vuln/detail/CVE-2018-14042', 'CVE-2016-10735': 'https://nvd.nist.gov/vuln/detail/CVE-2016-10735', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/twbs/bootstrap/issues/28236\nhttps://github.com/advisories/GHSA-pj7m-g53m-7638\nhttps://github.com/twbs/bootstrap/issues/20184\nhttps://github.com/advisories/GHSA-ph58-4vrj-w6hr\nhttps://github.com/twbs/bootstrap/issues/20631\nhttps://github.com/advisories/GHSA-4p24-vmcr-4gqj\nhttps://github.com/advisories/GHSA-9v3m-8fp8-mj99\nhttps://nvd.nist.gov/vuln/detail/CVE-2018-20676\n', 'solution': 'Please upgrade to the latest version of bootstrap.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '5191', 'alertRef': '10003'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1066', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '5192', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1060', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand

p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '5194', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1066', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '5197', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'cbhqk1udfl33y2lkmebsut4i', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1097', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '5199', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1060', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '5201', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',

'wascid': '15', '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.", 'messageId': '1060', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '5208', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1060', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '5210', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'CVE-2020-11023\nCVE-2020-11022\nCVE-2015-9251\nCVE-2019-11358\n', 'method': 'GET', 'evidence': 'jquery-2.1.1.min.js', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library jquery, version 2.1.1 is vulnerable.', 'messageId': '1060', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'CVE-2020-11023': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11023', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2020-11022': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11022', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CVE-2015-9251': 'https://nvd.nist.gov/vuln/detail/CVE-2015-9251', 'CVE-2019-11358': 'https://nvd.nist.gov/vuln/detail/CVE-2019-11358', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/jquery/jquery/issues/2432\nhttp://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/\nhttp://research.insecurelabs.org/jquery/test/\nhttps://blog.jquery.com/2019/04/10/jquery-3-4-0-released/\nhttps://nvd.nist.gov/vuln/detail/CVE-2019-11358\nhttps://github.com/advisories/GHSA-rmxg-73gg-4p98\nhttps://nvd.nist.gov/vuln/detail/CVE-2015-9251\nhttps://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b\nhttps://bugs.jquery.com/ticket/11974\nhttps://github.com/jquery/jquery.com/issues/162\nhttps://blog.jquery.com/2020/04/10/jquery-3-5-0-released/\n', 'solution': 'Please upgrade to the latest version of

jquery.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '5217', 'alertRef': '10003'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1070', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '5219', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1070', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '5226', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1070', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': ", 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '5234', 'alertRef': '10021'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1070', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(bdao5yxm2u3zuruls0xeem1z))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': ", 'attack': ", 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '5240', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'zh2frcg4h5kshxe3tv30wzrt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1064', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': ", 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '5243', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'zh2frcg4h5kshxe3tv30wzrt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1091', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': ", 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '5284', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1106', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session

Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '5308', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1114', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/play.png', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '5434', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=IXDIbZxB\npasswordParam=txtpwdcheck
\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST', 'evidence': 'txtpwdcheck',
'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.',
'messageId': '1117', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/', 'solution':
'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request
Identified', 'risk': 'Informational', 'id': '5508', 'alertRef': '10111'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'zh2frcg4h5kshxe3tv30wzrt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1139', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.min.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '5570', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'zh2frcg4h5kshxe3tv30wzrt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1142', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/bootstrap/css/responsive.css', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '5586', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'zh2frcg4h5kshxe3tv30wzrt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to

"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1148', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Script/jquery-1.9.1.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '5613', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'zh2frcg4h5kshxe3tv30wzrt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1151', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.min.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '5645', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'zh2frcg4h5kshxe3tv30wzrt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1182', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '5668', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=IeXyXPGh
\npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST',
'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.', 'messageId': '1140', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/',
'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request
Identified', 'risk': 'Informational', 'id': '5740', 'alertRef': '10111'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1204', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.min.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '5939', 'alertRef': '10112'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'zh2frcg4h5kshxe3tv30wzrt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1260', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/jquery.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6257', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'zh2frcg4h5kshxe3tv30wzrt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1265', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/psglogo.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6303', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'zh2frcg4h5kshxe3tv30wzrt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1284', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6337', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1285', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6418', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=GacHzSGj \npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST', 'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.', 'messageId': '1266', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/',

'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request Identified', 'risk': 'Informational', 'id': '6450', 'alertRef': '10111'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1267', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6454', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1289', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd?d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKxUvgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriYgReyv3ohx7-ei-o01&t=10c151ff', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6478', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=oNuiOFQe \npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST', 'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.', 'messageId': '1299', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request Identified', 'risk': 'Informational', 'id': '6580', 'alertRef': '10111'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1314', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6625', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'POST', 'evidence': 'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The

\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1318', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6684', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1321', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/psgtechlogo.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6718', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1322', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/play.png', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6725', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1335', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/css/responsive.css', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6726', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1344', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/bootstrap/js/sweetalert.min.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session

Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6753', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'zh2frcg4h5kshxe3tv30wzrt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1340', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/psgtechlogo.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6762', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1345', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6773', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1349', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.min.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6776', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1374', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6806', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1370',

'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(l2lxutmdudadxiw3lyx3vavf))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '6943', 'alertRef': '10036'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'w4xqe0diuwhghxfb4ijyd2h0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1402', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/icon', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '6949', 'alertRef': '10112'}

{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '1370', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(l2lxutmdudadxiw3lyx3vavf))/FbkWfLogin.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '6950', 'alertRef': '10061'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '1372', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header', 'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id': '6954', 'alertRef': '10020-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525', 'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.', 'messageId': '1372', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/FbkWfLogin.aspx', 'tags': {'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-recommendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control', 'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '6957', 'alertRef': '10015'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1370', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(l2lxutmdudadxiw3lyx3vavf))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '6959', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '1372', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w

3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '6963', 'alertRef': '10038-1'}

{'sourceid': '3', 'other': '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: "__VIEWSTATE" "__VIEWSTATEGENERATOR" "txtpwd" "TxtRollNo"].', 'method': 'GET', 'evidence': '<form method="post" action="./FbkWfLogin.aspx" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '1372', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '6973', 'alertRef': '10202'}

{'sourceid': '3', 'other': 'The following pattern was used: \\bUSER\\b and was detected in the element starting with: "<script type="text/javascript">\r\n\r\n \r\n\r\n $(document).ready(function () {\r\n \r\n \r\n //", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'User', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1372', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '6977', 'alertRef': '10027'}

{'sourceid': '3', 'other': 'No links have been found while there are scripts, which is an indication that this is a modern web application.', 'method': 'GET', 'evidence': '<script src="bootstrap/js/jquery-2.1.1.min.js"></script>', 'pluginId': '10109', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1', '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.', 'messageId': '1372', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/FbkWfLogin.aspx', 'tags': {}, 'reference': '', 'solution': 'This is an informational alert and so no changes are required.', 'alert': 'Modern Web Application', 'param': '', 'attack': '', 'name': 'Modern Web Application', 'risk': 'Informational', 'id': '6980', 'alertRef': '10109'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1372', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '6985', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1379', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your

web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '6989', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1372', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '6991', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1379', 'inputVector': '', 'url': '
https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/bootstrap.min.j
s', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '6993', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method':
'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14',
'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response
header field(s).', 'messageId': '1372', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/FbkWfLogin.aspx', 'tags':
{'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933':
'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varun
m/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not
return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name':
'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '6996', 'alertRef': '10061'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '1379', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '6997', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1372', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7002', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1379', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht

ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7005', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1372', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7010', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'CVE-2018-14041\nCVE-2019-8331\nCVE-2018-20677\nCVE-2018-20676\nCV
E-2018-14042\nCVE-2016-10735\n', 'method': 'GET', 'evidence': '* Bootstrap v3.3.7', 'pluginId': '10003',
'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library bootstrap, version
3.3.7 is vulnerable.', 'messageId': '1379', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(
S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/bootstrap.min.js', 'tags': {'CVE-2018-14041':
'https://nvd.nist.gov/vuln/detail/CVE-2018-14041', 'CVE-2019-8331':
'https://nvd.nist.gov/vuln/detail/CVE-2019-8331', 'OWASP_2017_A09': 'https://owasp.org/www-project-t
op-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2018-20677':
'https://nvd.nist.gov/vuln/detail/CVE-2018-20677', 'CVE-2018-20676':
'https://nvd.nist.gov/vuln/detail/CVE-2018-20676', 'CVE-2018-14042':
'https://nvd.nist.gov/vuln/detail/CVE-2018-14042', 'CVE-2016-10735':
'https://nvd.nist.gov/vuln/detail/CVE-2016-10735', 'OWASP_2021_A06':
'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CWE-829':
'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/twbs/bootstrap/issues/2
8236\nhttps://github.com/advisories/GHSA-pj7m-g53m-7638\nhttps://github.com/twbs/bootstrap/issues
/20184\nhttps://github.com/advisories/GHSA-ph58-4vrj-w6hr\nhttps://github.com/twbs/bootstrap/issues/
20631\nhttps://github.com/advisories/GHSA-4p24-vmcr-4gqj\nhttps://github.com/advisories/GHSA-9v3
m-8fp8-mj99\nhttps://nvd.nist.gov/vuln/detail/CVE-2018-20676\n', 'solution': 'Please upgrade to the
latest version of bootstrap.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS
Library', 'risk': 'Medium', 'id': '7011', 'alertRef': '10003'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1382',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstr
ap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/

```
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '7012', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1382', 'inputVector': '', 'url': '
https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/css/bootstrap.min
.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7017', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'POST', 'evidence':
'2mfipee0te03q20se1nfmkte', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1410', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '7019', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1386',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstr
ap/css/ecampus.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '7020', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1385',
```

'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '7021', 'alertRef': '10036'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1382', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7022', 'alertRef': '10021'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bDB\\b and was detected 2 times, the first in the element starting with: "!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.docu", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'db', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1384', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '7025', 'alertRef': '10027'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1386', 'inputVector': '', 'url': '
https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/css/ecampus.css'
, 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7027', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1385', 'inputVector': '', 'url': '
https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/sweetalert.min.j
s', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7028', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1382', 'inputVector': '', 'url': 'https:
//ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/css/bootstrap.min.css',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7030', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the
element starting with: "},removeAttr:function(a,b){var
c,d,e=0,f=b&&b.match(E);if(f&&1===a.nodeType)while(c=f[e++])d=n.propFix[c]||c,n.expr.match.bool.t",
see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'username',
'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears

to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1384', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '7032', 'alertRef': '10027'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1388', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '7033', 'alertRef': '10036'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1386', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7034', 'alertRef': '10021'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1385', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7036', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1384', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '7037', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1388', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',

'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7038', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1386', 'inputVector': '', 'url': 'https:
//ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/css/ecampus.css',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7041', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1385', 'inputVector': '', 'url': 'https:
//ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/sweetalert.min.js',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7043', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1384', 'inputVector': '', 'url': '
https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/jquery-2.1.1.mi
n.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7044', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1411', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfLoginPage.aspx', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '7045', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1389', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '7047', 'alertRef': '10036'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1388', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7048', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1390', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '7052', 'alertRef': '10036'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1384', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7053', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1388', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to

suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': ", 'attack': ", 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7054', 'alertRef': '10037'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': ", 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1389', 'inputVector': ", 'url': '
https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/css/sweetalert.cs
s', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': ", 'attack': ",
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7055', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': ", 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1390', 'inputVector': ", 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/Images/psg_tech.jpg',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': ", 'attack': ",
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7060', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1384', 'inputVector': ", 'url': 'https:
//ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/jquery-2.1.1.min.js',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': ", 'attack': ", 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7061', 'alertRef': '10037'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1389', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7062', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1390', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7067', 'alertRef': '10021'}
{'sourceid': '3', 'other': 'CVE-2020-11023\nCVE-2020-11022\nCVE-2015-9251\nCVE-2019-11358\n', 'method': 'GET', 'evidence': 'jquery-2.1.1.min.js', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library jquery, version 2.1.1 is vulnerable.', 'messageId': '1384', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'CVE-2020-11023': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11023', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2020-11022': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11022', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CVE-2015-9251': 'https://nvd.nist.gov/vuln/detail/CVE-2015-9251', 'CVE-2019-11358': 'https://nvd.nist.gov/vuln/detail/CVE-2019-11358', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/jquery/jquery/issues/24

32\nhttp://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/\nhttp://research.insecurelabs.org/jquery/test/\nhttps://blog.jquery.com/2019/04/10/jquery-3-4-0-released/\nhttps://nvd.nist.gov/vuln/detail/CVE-2019-11358\nhttps://github.com/advisories/GHSA-rmxg-73gg-4p98\nhttps://nvd.nist.gov/vuln/detail/CVE-2015-9251\nhttps://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b\nhttps://bugs.jquery.com/ticket/11974\nhttps://github.com/jquery/jquery.com/issues/162\nhttps://blog.jquery.com/2020/04/10/jquery-3-5-0-released/\n', 'solution': 'Please upgrade to the latest version of jquery.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '7068', 'alertRef': '10003'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1389', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7069', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1390', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7074', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '1396', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/icon/apple-touch-icon.jpg',

```
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '7083', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1419', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '7087', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1396',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/icon/apple-touch-icon.jpg',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '7092', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1396', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/icon/apple-touch-icon.jpg',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
```

'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7098', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1396', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(xa2uwebeddqunubrselqkvm5))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7108', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'zh2frcg4h5kshxe3tv30wzrt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1424', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '7154', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1422', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/psgtechlogo.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '7239', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1425', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/psgtechlogo.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session

Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '7260', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'zh2frcg4h5kshxe3tv30wzrt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1434', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/modernizr-2.5.3.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '7279', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1471', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/psglogo.jpg', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '7433', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1488', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/Images', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '7438', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence':
'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy
with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.",
'messageId': '1456', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021':
'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference':
'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern
Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one
of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header',

'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id': '7440', 'alertRef': '10020-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525', 'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.', 'messageId': '1456', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/FbkWfLogin.aspx', 'tags': {'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-recommendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control', 'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '7457', 'alertRef': '10015'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '1456', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '7458', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1489', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.min.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '7461', 'alertRef': '10112'}
{'sourceid': '3', 'other': '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: "__VIEWSTATE" "__VIEWSTATEGENERATOR" "txtpwd" "TxtRollNo"].', 'method': 'GET', 'evidence':

'<form method="post" action="./FbkWfLogin.aspx" id="form1">', 'pluginId': '10202', 'cweid': '352', 'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a number of situations, including:\n * The victim has an active session on the target site.\n * The victim is authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target site.\n\nCSRF 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.", 'messageId': '1456', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '7470', 'alertRef': '10202'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1466', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your

web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': ", 'attack': ", 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '7473', 'alertRef': '10036'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': ", 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1466', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': ", 'attack': ", 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7479', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSER\\b and was detected in the element starting with: "<script type="text/javascript">\r\n\r\n \r\n\r\n $(document).ready(function () {\r\n \r\n \r\n //", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'User', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1456', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': ", 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': ", 'attack': ", 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '7481', 'alertRef': '10027'}
{'sourceid': '3', 'other': 'No links have been found while there are scripts, which is an indication that this is a modern web application.', 'method': 'GET', 'evidence': '<script src="bootstrap/js/jquery-2.1.1.min.js"></script>', 'pluginId': '10109', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1', '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.', 'messageId': '1456', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/FbkWfLogin.aspx', 'tags': {}, 'reference': ", 'solution': 'This is an informational alert and so no changes are required.', 'alert': 'Modern Web Application', 'param': ", 'attack': ", 'name': 'Modern Web Application', 'risk': 'Informational', 'id': '7486', 'alertRef': '10109'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1490', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/_references.js', 'tags': {}, 'reference':

'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '7489', 'alertRef': '10112'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1466', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7492', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1456', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '7493', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1456', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt

ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7499', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1466', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7500', 'alertRef': '10037'}

{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '1456', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/FbkWfLogin.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '7505', 'alertRef': '10061'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1473', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header

Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '7509', 'alertRef': '10036'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1456', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7510', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1474', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '7511', 'alertRef': '10036'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1494', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/icon', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '7512', 'alertRef': '10112'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1456', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7516', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1473', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7517', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1474', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7519', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bDB\\b and was detected 2 times, the first in the element starting with: "!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.docu", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'db', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments

which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1476', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '7523', 'alertRef': '10027'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1473', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7526', 'alertRef': '10021'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1474', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.'', 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7529', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1473', 'inputVector': '', 'url': 'https:
//ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/js/bootstrap.min.js',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7532', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1474', 'inputVector': '', 'url': 'https:
//ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/sweetalert.css',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7533', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the
element starting with: ''},removeAttr:function(a,b){var
c,d,e=0,f=b&&b.match(E);if(f&&1===a.nodeType)while(c=f[e++])d=n.propFix[c]||c,n.expr.match.bool.t'',
see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'username',
'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears
to contain suspicious comments which may help an attacker. Note: Matches made within script blocks
or files are against the entire content not only comments.', 'messageId': '1476', 'inputVector': '', 'url': 'htt
ps://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/js/jquery-2.1.1.min.j
s', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leaka
ge', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that

```
return information that may help an attacker and fix any underlying problems they refer to.', 'alert':
'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure -
Suspicious Comments', 'risk': 'Informational', 'id': '7535', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1480',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/w3.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '7538', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1480', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/w3.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7540', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1476',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootst
rap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '7544', 'alertRef': '10036'}
```

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': ", 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1480', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': ", 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7547', 'alertRef': '10021'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': ", 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1476', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': ", 'attack': ", 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7548', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1480', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP

Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7549', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'CVE-2018-14041\nCVE-2019-8331\nCVE-2018-20677\nCVE-2018-20676\nCV
E-2018-14042\nCVE-2016-10735\n', 'method': 'GET', 'evidence': '* Bootstrap v3.3.7', 'pluginId': '10003',
'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library bootstrap, version
3.3.7 is vulnerable.', 'messageId': '1473', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(
S(qf2m0g43uom422ppjqwavqe3))/bootstrap/js/bootstrap.min.js', 'tags': {'CVE-2018-14041':
'https://nvd.nist.gov/vuln/detail/CVE-2018-14041', 'CVE-2019-8331':
'https://nvd.nist.gov/vuln/detail/CVE-2019-8331', 'OWASP_2017_A09': 'https://owasp.org/www-project-t
op-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2018-20677':
'https://nvd.nist.gov/vuln/detail/CVE-2018-20677', 'CVE-2018-20676':
'https://nvd.nist.gov/vuln/detail/CVE-2018-20676', 'CVE-2018-14042':
'https://nvd.nist.gov/vuln/detail/CVE-2018-14042', 'CVE-2016-10735':
'https://nvd.nist.gov/vuln/detail/CVE-2016-10735', 'OWASP_2021_A06':
'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CWE-829':
'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/twbs/bootstrap/issues/2
8236\nhttps://github.com/advisories/GHSA-pj7m-g53m-7638\nhttps://github.com/twbs/bootstrap/issues
/20184\nhttps://github.com/advisories/GHSA-ph58-4vrj-w6hr\nhttps://github.com/twbs/bootstrap/issues/
20631\nhttps://github.com/advisories/GHSA-4p24-vmcr-4gqj\nhttps://github.com/advisories/GHSA-9v3
m-8fp8-mj99\nhttps://nvd.nist.gov/vuln/detail/CVE-2018-20676\n', 'solution': 'Please upgrade to the
latest version of bootstrap.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS
Library', 'risk': 'Medium', 'id': '7550', 'alertRef': '10003'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '1476',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootst
rap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7553', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1476', 'inputVector': '', 'url': 'https:
//ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/js/jquery-2.1.1.min.js',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',

'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7554', 'alertRef': '10037'}

{'sourceid': '3', 'other': 'CVE-2020-11023\nCVE-2020-11022\nCVE-2015-9251\nCVE-2019-11358\n', 'method': 'GET', 'evidence': 'jquery-2.1.1.min.js', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library jquery, version 2.1.1 is vulnerable.', 'messageId': '1476', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'CVE-2020-11023': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11023', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2020-11022': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11022', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CVE-2015-9251': 'https://nvd.nist.gov/vuln/detail/CVE-2015-9251', 'CVE-2019-11358': 'https://nvd.nist.gov/vuln/detail/CVE-2019-11358', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/jquery/jquery/issues/2432\nhttp://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/\nhttp://research.insecurelabs.org/jquery/test/\nhttps://blog.jquery.com/2019/04/10/jquery-3-4-0-released/\nhttps://nvd.nist.gov/vuln/detail/CVE-2019-11358\nhttps://github.com/advisories/GHSA-rmxg-73gg-4p98\nhttps://nvd.nist.gov/vuln/detail/CVE-2015-9251\nhttps://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b\nhttps://bugs.jquery.com/ticket/11974\nhttps://github.com/jquery/jquery.com/issues/162\nhttps://blog.jquery.com/2020/04/10/jquery-3-5-0-released/\n', 'solution': 'Please upgrade to the latest version of jquery.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '7555', 'alertRef': '10003'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1486', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '7561', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1484', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':

'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '7563', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1486', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7568', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1484', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7569', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1484', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':

'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7576', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1486', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7577', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1486', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7580', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1484', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7582', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '1491', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '7586', 'alertRef': '10038-1'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1491', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '7588', 'alertRef': '10036'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'gnlo0ia2wms1a4bombrlfvql', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',

'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1506', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '7589', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1481',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootst
rap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '7594', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1491', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/icon/apple-touch-icon.jpg',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7596', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1491', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/icon/apple-touch-icon.jpg',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit

y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7604', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1481', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '7611', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1498', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '7623', 'alertRef': '10112'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1481', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':

'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '7624', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1481', 'inputVector': '', 'url': 'https:
//ecampus.psgtech.ac.in/feedback/(S(qf2m0g43uom422ppjqwavqe3))/bootstrap/css/bootstrap.min.css',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '7628', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=jhpPnnKO
\npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST',
'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.', 'messageId': '1496', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/',
'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request
Identified', 'risk': 'Informational', 'id': '7658', 'alertRef': '10111'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cohtcorufno55p3lcppeaqg5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1536', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '7733', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1539', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/_references.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session

Management Response Identified', 'risk': 'Informational', 'id': '7762', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cohtcorufno55p3lcppeaqg5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1515', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '7788', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1544', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '7796', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cohtcorufno55p3lcppeaqg5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1546', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd
?d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKx
UvgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriY
gReyv3ohx7-ei-o01&t=10c151ff', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '7854', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1568', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/style.css', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '7900', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cohtcorufno55p3lcppeaqg5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session

```
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1553', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd
?d=geiJw278ELCE4oVrRV2zHxl4wPiCyAyFHHfDFzBwX9Hp7XbtV3NCf3xuCpzPTnIRW2dJvayOXQq
OoSXyt8im1TzMRVB0IuHKFJU24PVx4BTHjdtmWWkIrjaXmOc8s0R8UPDzpkdImHC-ll2ojyANip2Z-su
FTjJXCyu_H-il4yDEOHJiEVBhwuI32VFkf50c0&t=10c151ff', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '8046', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cohtcorufno55p3lcppeaqg5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1593', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/bootstrap/css/responsive.css', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '8146', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cohtcorufno55p3lcppeaqg5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1598', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.min.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '8171', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cohtcorufno55p3lcppeaqg5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1612', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '8200', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1628',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(v2rgv1a5idt3aw0fbdkedt5r))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
```

'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '8348', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '1628', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(v2rgv1a5idt3aw0fbdkedt5r))/FbkWfLogin.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '8351', 'alertRef': '10061'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1634', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '8355', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence': 'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.", 'messageId': '1631', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021': 'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one

of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header',
'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id':
'8356', 'alertRef': '10020-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1628', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(v2rgv1a5idt3aw0fbdkedt5r))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '8357', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1638', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '8359', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1634', 'inputVector': '', 'url': '
https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js/sweetalert.min.j
s', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '8361', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',

'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1643', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '8363', 'alertRef': '10112'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1634', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '8364', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525', 'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.', 'messageId': '1631', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/FbkWfLogin.aspx', 'tags': {'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-recommendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control', 'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '8367', 'alertRef': '10015'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1634', 'inputVector': '', 'url': 'https:

//ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js/sweetalert.min.js',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '8368', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '1631', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '8369', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '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:
"__VIEWSTATE" "__VIEWSTATEGENERATOR" "txtpwd" "TxtRollNo"].', 'method': 'GET', 'evidence':
'<form method="post" action="./FbkWfLogin.aspx" id="form1">', 'pluginId': '10202', 'cweid': '352',
'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission
form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request
to a target destination without their knowledge or intent in order to perform an action as the victim. The
underlying cause is application functionality using predictable URL/form actions in a repeatable way.
The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast,
cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are
not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF,
one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a
number of situations, including:\n * The victim has an active session on the target site.\n * The victim is
authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target
site.\n\nCSRF 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.", 'messageId': '1631', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/FbkWfLogin.aspx', 'tags':

{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery', 'OWASP_2017_A05': 'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352': 'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitions/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase: Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and Design\nGenerate 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).\nNote that this can be bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '8371', 'alertRef': '10202'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1646', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/css/sweetalert.css', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '8374', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSER\\b and was detected in the element starting with: "<script type="text/javascript">\r\n\r\n \r\n\r\n $(document).ready(function () {\r\n \r\n \r\n //", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'User', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1631', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '8375', 'alertRef': '10027'}
{'sourceid': '3', 'other': 'No links have been found while there are scripts, which is an indication that this is a modern web application.', 'method': 'GET', 'evidence': '<script

src="bootstrap/js/jquery-2.1.1.min.js"></script>', 'pluginId': '10109', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1', '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.', 'messageId': '1631', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/FbkWfLogin.aspx', 'tags': {}, 'reference': '', 'solution': 'This is an informational alert and so no changes are required.', 'alert': 'Modern Web Application', 'param': '', 'attack': '', 'name': 'Modern Web Application', 'risk': 'Informational', 'id': '8377', 'alertRef': '10109'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1631', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '8379', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1631', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '8380', 'alertRef': '10035-1'}

{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method': 'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14', 'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response header field(s).', 'messageId': '1631', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/FbkWfLogin.aspx', 'tags': {'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933': 'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not

return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name': 'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '8382', 'alertRef': '10061'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'cohtcorufno55p3lcppeaqg5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1648', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Images/psgtechlogo.jpg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '8383', 'alertRef': '10112'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1631', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '8384', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1631', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"

HTTP Response Header Field(s)', 'risk': 'Low', 'id': '8385', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': '3wil5laqvw1s45m4lby21ht5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1655', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/icon', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '8386', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1642', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '8388', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1639', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '8389', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1641', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstr

ap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '8390', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1646',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstr
ap/css/sweetalert.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '8392', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1642', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/css/w3.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '8394', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1639', 'inputVector': '', 'url': '
https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/css/ecampus.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt

```
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '8395', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1646', 'inputVector': '', 'url': '
https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/css/sweetalert.css
', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '8397', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1641', 'inputVector': '', 'url': '
https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js/bootstrap.min.js'
, 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '8398', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '1639',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstr
ap/css/ecampus.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
```

X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '8399', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '1642',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/css/w3.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '8401', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '1646',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstr
ap/css/sweetalert.css', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '8402', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1639', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '8403', 'alertRef': '10037'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1641', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '8406', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1646', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"

HTTP Response Header Field(s)', 'risk': 'Low', 'id': '8407', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1642', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '8408', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bDB\\b and was detected 2 times, the first in the element starting with: "!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.docu", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'db', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1643', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '8409', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1645', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '8410', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1641', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '8412', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the element starting with: "},removeAttr:function(a,b){var c,d,e=0,f=b&&b.match(E);if(f&&1===a.nodeType)while(c=f[e++])d=n.propFix[c]||c,n.expr.match.bool.t", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'username', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1643', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '8417', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1649', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '8421', 'alertRef': '10036'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1645', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '8422', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1643', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '8424', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'CVE-2018-14041\nCVE-2019-8331\nCVE-2018-20677\nCVE-2018-20676\nCVE-2018-14042\nCVE-2016-10735\n', 'method': 'GET', 'evidence': '* Bootstrap v3.3.7', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library bootstrap, version 3.3.7 is vulnerable.', 'messageId': '1641', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js/bootstrap.min.js', 'tags': {'CVE-2018-14041': 'https://nvd.nist.gov/vuln/detail/CVE-2018-14041', 'CVE-2019-8331': 'https://nvd.nist.gov/vuln/detail/CVE-2019-8331', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2018-20677': 'https://nvd.nist.gov/vuln/detail/CVE-2018-20677', 'CVE-2018-20676': 'https://nvd.nist.gov/vuln/detail/CVE-2018-20676', 'CVE-2018-14042': 'https://nvd.nist.gov/vuln/detail/CVE-2018-14042', 'CVE-2016-10735': 'https://nvd.nist.gov/vuln/detail/CVE-2016-10735', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/twbs/bootstrap/issues/28236\nhttps://github.com/advisories/GHSA-pj7m-g53m-7638\nhttps://github.com/twbs/bootstrap/issues/20184\nhttps://github.com/advisories/GHSA-ph58-4vrj-w6hr\nhttps://github.com/twbs/bootstrap/issues/20631\nhttps://github.com/advisories/GHSA-4p24-vmcr-4gqj\nhttps://github.com/advisories/GHSA-9v3m-8fp8-mj99\nhttps://nvd.nist.gov/vuln/detail/CVE-2018-20676\n', 'solution': 'Please upgrade to the latest version of bootstrap.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '8428', 'alertRef': '10003'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1649', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '8429', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1643', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '8430', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1649', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '8431', 'alertRef': '10021'}

{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1645', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '8437', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1645', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '8439', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1649', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We

b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '8440', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '1652', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/icon/apple-touch-icon.jpg',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '8444', 'alertRef': '10038-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '1643',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstr
ap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05':
'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '8445', 'alertRef': '10021'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cohtcorufno55p3lcppeaqg5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1686', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/script.js', 'tags': {},

```
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '8447', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1643', 'inputVector': '', 'url': 'https:
//ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstrap/js/jquery-2.1.1.min.js',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '8450', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1652',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/icon/apple-touch-icon.jpg',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '8451', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1652', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/icon/apple-touch-icon.jpg',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
```

```
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '8458', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'CVE-2020-11023\nCVE-2020-11022\nCVE-2015-9251\nCVE-2019-11358\n',
'method': 'GET', 'evidence': 'jquery-2.1.1.min.js', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium',
'wascid': '-1', 'description': 'The identified library jquery, version 2.1.1 is vulnerable.', 'messageId': '1643',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/bootstr
ap/js/jquery-2.1.1.min.js', 'tags': {'CVE-2020-11023': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11023',
'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_
Known_Vulnerabilities.html', 'CVE-2020-11022': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11022',
'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/',
'CVE-2015-9251': 'https://nvd.nist.gov/vuln/detail/CVE-2015-9251', 'CVE-2019-11358':
'https://nvd.nist.gov/vuln/detail/CVE-2019-11358', 'CWE-829':
'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/jquery/jquery/issues/24
32\nhttp://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/\nhttp://research.insecurelabs.org/
jquery/test/\nhttps://blog.jquery.com/2019/04/10/jquery-3-4-0-released/\nhttps://nvd.nist.gov/vuln/detail/
CVE-2019-11358\nhttps://github.com/advisories/GHSA-rmxg-73gg-4p98\nhttps://nvd.nist.gov/vuln/deta
il/CVE-2015-9251\nhttps://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd08086
19b1b\nhttps://bugs.jquery.com/ticket/11974\nhttps://github.com/jquery/jquery.com/issues/162\nhttps://
blog.jquery.com/2020/04/10/jquery-3-5-0-released/\n', 'solution': 'Please upgrade to the latest version of
jquery.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk':
'Medium', 'id': '8460', 'alertRef': '10003'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1652', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(stu5dd33dawhhlmwelaltmw4))/icon/apple-touch-icon.jpg',
'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '8465', 'alertRef': '10037'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cohtcorufno55p3lcppeaqg5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1701', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/psglogo.jpg', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '8547', 'alertRef': '10112'}
{'sourceid': '3', 'other': 'userParam=txtusercheck\nuserValue=UoDBVSZO
\npasswordParam=txtpwdcheck\nreferer=https://ecampus.psgtech.ac.in/studzone2/', 'method': 'POST',
'evidence': 'txtpwdcheck', 'pluginId': '10111', 'cweid': '-1', 'confidence': 'Low', 'wascid': '-1', '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.', 'messageId': '1699', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Authentication Request Identified', 'param': 'txtusercheck', 'attack': '', 'name': 'Authentication Request Identified', 'risk': 'Informational', 'id': '8750', 'alertRef': '10111'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1730', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/play.png', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '8917', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'cohtcorufno55p3lcppeaqg5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1723', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/data1/images/psg_tech.jpeg', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '8920', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1750', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '8923', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'hse0dpjah02z2ckuhvpxnmkp', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1', 'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1756', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.min.js', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session

Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9000', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10020', 'cweid': '1021', 'confidence':
'Medium', 'wascid': '15', 'description': "The response does not include either Content-Security-Policy
with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.",
'messageId': '1766', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-1021':
'https://cwe.mitre.org/data/definitions/1021.html', 'WSTG-v42-CLNT-09': 'https://owasp.org/www-project
-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testin
g_for_Clickjacking', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference':
'https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options', 'solution': 'Modern
Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one
of them is set on all web pages returned by your site/app.\nIf 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.', 'alert': 'Missing Anti-clickjacking Header',
'param': 'x-frame-options', 'attack': '', 'name': 'Missing Anti-clickjacking Header', 'risk': 'Medium', 'id':
'9087', 'alertRef': '10020-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'private', 'pluginId': '10015', 'cweid': '525',
'confidence': 'Low', 'wascid': '13', 'description': 'The cache-control header has not been set properly or is
missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files
this might be intended, however, the resources should be reviewed to ensure that no sensitive content
will be cached.', 'messageId': '1766', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/FbkWfLogin.aspx', 'tags':
{'CWE-525': 'https://cwe.mitre.org/data/definitions/525.html', 'WSTG-v42-ATHN-06': 'https://owasp.org/
www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_T
esting/06-Testing_for_Browser_Cache_Weaknesses'}, 'reference': 'https://cheatsheetseries.owasp.org/
cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching\nhttps://developer.mozilla
.org/en-US/docs/Web/HTTP/Headers/Cache-Control\nhttps://grayduck.mn/2021/09/13/cache-control-re
commendations/', 'solution': 'For secure content, ensure the cache-control HTTP header is set with
"no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives
"public, max-age, immutable".', 'alert': 'Re-examine Cache-control Directives', 'param': 'cache-control',
'attack': '', 'name': 'Re-examine Cache-control Directives', 'risk': 'Informational', 'id': '9090', 'alertRef':
'10015'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence':
'High', 'wascid': '15', '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.', 'messageId': '1766', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps:
//cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w
3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.co
m/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web
server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.',

```
'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security
Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '9099', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1770',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/sweetalert.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '9101', 'alertRef': '10036'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1783', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/Images', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9105', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1770', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/sweetalert.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '9106', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '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:
"__VIEWSTATE" "__VIEWSTATEGENERATOR" "txtpwd" "TxtRollNo" ].', 'method': 'GET', 'evidence':
'<form method="post" action="./FbkWfLogin.aspx" id="form1">', 'pluginId': '10202', 'cweid': '352',
'confidence': 'Low', 'wascid': '9', 'description': "No Anti-CSRF tokens were found in a HTML submission
```

form.\nA cross-site request forgery is an attack that involves forcing a victim to send an HTTP request
to a target destination without their knowledge or intent in order to perform an action as the victim. The
underlying cause is application functionality using predictable URL/form actions in a repeatable way.
The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast,
cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are
not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF,
one-click attack, session riding, confused deputy, and sea surf.\n\nCSRF attacks are effective in a
number of situations, including:\n * The victim has an active session on the target site.\n * The victim is
authenticated via HTTP auth on the target site.\n * The victim is on the same local network as the target
site.\n\nCSRF 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.", 'messageId': '1766', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-SESS-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/06-Session_Management_Testing/05-Testing_for_Cross_Site_Request_Forgery',
'OWASP_2017_A05':
'https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html', 'CWE-352':
'https://cwe.mitre.org/data/definitions/352.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheats
heets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html\nhttps://cwe.mitre.org/data/definitio
ns/352.html', 'solution': 'Phase: Architecture and Design\nUse a vetted library or framework that does
not allow this weakness to occur or provides constructs that make this weakness easier to avoid.\nFor
example, use anti-CSRF packages such as the OWASP CSRFGuard.\n\nPhase:
Implementation\nEnsure that your application is free of cross-site scripting issues, because most CSRF
defenses can be bypassed using attacker-controlled script.\n\nPhase: Architecture and
Design\nGenerate 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).\nNote that this can be
bypassed using XSS.\n\nIdentify 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.\nNote that this can be bypassed using XSS.\n\nUse the ESAPI Session Management
control.\nThis control includes a component for CSRF.\n\nDo not use the GET method for any request
that triggers a state change.\n\nPhase: Implementation\nCheck 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.', 'alert': 'Absence of Anti-CSRF
Tokens', 'param': '', 'attack': '', 'name': 'Absence of Anti-CSRF Tokens', 'risk': 'Medium', 'id': '9111',
'alertRef': '10202'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '1770',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/sweetalert.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g

g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': ", 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '9113', 'alertRef': '10021'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSER\\b and was detected in the element starting with: "<script type="text/javascript">\r\n\r\n \r\n\r\n $(document).ready(function () {\r\n \r\n \r\n //", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'User', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1766', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/FbkWfLogin.aspx', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': ", 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': ", 'attack': ", 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '9114', 'alertRef': '10027'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1770', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/sweetalert.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': ", 'attack': ", 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '9115', 'alertRef': '10037'}
{'sourceid': '3', 'other': 'No links have been found while there are scripts, which is an indication that this is a modern web application.', 'method': 'GET', 'evidence': '<script src="bootstrap/js/jquery-2.1.1.min.js"></script>', 'pluginId': '10109', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1', '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.', 'messageId': '1766', 'inputVector': ", 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/FbkWfLogin.aspx', 'tags': {}, 'reference': ", 'solution': 'This is an informational alert and so no changes are required.', 'alert': 'Modern Web Application', 'param': ", 'attack': ", 'name': 'Modern Web Application', 'risk': 'Informational', 'id': '9116', 'alertRef': '10109'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1766',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '9117', 'alertRef': '10036'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1787', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/icon', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9118', 'alertRef': '10112'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1766', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '9119', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': 'An attacker can use this information to exploit known vulnerabilities.', 'method':
'GET', 'evidence': '4.0.30319', 'pluginId': '10061', 'cweid': '933', 'confidence': 'High', 'wascid': '14',
'description': 'Server leaks information via "X-AspNet-Version"/"X-AspNetMvc-Version" HTTP response
header field(s).', 'messageId': '1766', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/FbkWfLogin.aspx', 'tags':
{'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-933':
'https://cwe.mitre.org/data/definitions/933.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt

ps://www.troyhunt.com/shhh-dont-let-your-response-headers/\nhttps://blogs.msdn.microsoft.com/varun
m/2013/04/23/remove-unwanted-http-response-headers/', 'solution': 'Configure the server so it will not
return those headers.', 'alert': 'X-AspNet-Version Response Header', 'param': '', 'attack': '', 'name':
'X-AspNet-Version Response Header', 'risk': 'Low', 'id': '9120', 'alertRef': '10061'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '1766',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '9121', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1766', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/FbkWfLogin.aspx', 'tags':
{'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',
'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework',
'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '9122', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1781',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/Images/psg_tech.jpg', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',

```
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '9125', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1779',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/ecampus.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '9126', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1776',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/sweetalert.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '9127', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1781', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/Images/psg_tech.jpg', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
```

```
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '9129', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1774',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/w3.css', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your
web server, application server, load balancer, etc. is configured to suppress the "Server" header or
provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header
Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response
Header Field', 'risk': 'Low', 'id': '9130', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1779', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/ecampus.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '9132', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1776', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/sweetalert.css',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
```

Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '9133', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence':
'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy
mechanism whereby a web server declares that complying user agents (such as a web browser) are to
interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an
IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1774', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/w3.css', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319':
'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhtt
ps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transpo
rt_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797',
'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce
Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '',
'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '9134', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server
error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium',
'wascid': '15', '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.", 'messageId': '1781',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/Images/psg_tech.jpg', 'tags':
{'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693':
'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'htt
ps://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/g
g622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the
application/web server sets the Content-Type header appropriately, and that it sets the
X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert':
'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name':
'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '9135', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200',
'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1773',
'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/bootstrap.min.js',
'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/',
'OWASP_2017_A06':
'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html',
'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati
on_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/
core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pand
p.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your

web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '9137', 'alertRef': '10036'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1779', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '9138', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1781', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/Images/psg_tech.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '9139', 'alertRef': '10037'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1776',

'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '9140', 'alertRef': '10021'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1774', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '9141', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1773', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '9143', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1779', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/ecampus.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '9144', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1776', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/sweetalert.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '9145', 'alertRef': '10037'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1774', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/w3.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '9146', 'alertRef': '10037'}

{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence': 'tby4vwb5fzdp2wwkwgiukbnt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',

'description': 'The given response has been identified as containing a session management token. The \'Other Info\' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.', 'messageId': '1796', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/', 'tags': {}, 'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session Management Response Identified', 'risk': 'Informational', 'id': '9147', 'alertRef': '10112'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1773', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '9150', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1780', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '9151', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10038', 'cweid': '693', 'confidence': 'High', 'wascid': '15', '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.', 'messageId': '1785', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy\nhttps://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html\nhttps://www.w3.org/TR/CSP/\nhttps://w3c.github.io/webappsec-csp/\nhttps://web.dev/articles/csp\nhttps://caniuse.com/#feat=contentsecuritypolicy\nhttps://content-security-policy.com/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.', 'alert': 'Content Security Policy (CSP) Header Not Set', 'param': '', 'attack': '', 'name': 'Content Security Policy (CSP) Header Not Set', 'risk': 'Medium', 'id': '9153', 'alertRef': '10038-1'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bDB\\b and was detected 2 times, the first in the element starting with: "!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.docu", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'db', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1777', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '9156', 'alertRef': '10027'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1780', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '9157', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1773', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/bootstrap.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Applicati

on_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '9158', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1785', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '9162', 'alertRef': '10036'}
{'sourceid': '3', 'other': 'The following pattern was used: \\bUSERNAME\\b and was detected in the element starting with: "},removeAttr:function(a,b){var c,d,e=0,f=b&&b.match(E);if(f&&1===a.nodeType)while(c=f[e++])d=n.propFix[c]||c,n.expr.match.bool.t", see evidence field for the suspicious comment/snippet.', 'method': 'GET', 'evidence': 'username', 'pluginId': '10027', 'cweid': '200', 'confidence': 'Low', 'wascid': '13', 'description': 'The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.', 'messageId': '1777', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-05': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': '', 'solution': 'Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.', 'alert': 'Information Disclosure - Suspicious Comments', 'param': '', 'attack': '', 'name': 'Information Disclosure - Suspicious Comments', 'risk': 'Informational', 'id': '9164', 'alertRef': '10027'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1780', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '9165', 'alertRef': '10021'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1785', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '9167', 'alertRef': '10035-1'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1777', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '9169', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1780', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/css/bootstrap.min.css', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/',

'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '9172', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1785', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/icon/apple-touch-icon.jpg', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '9174', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': '', 'pluginId': '10035', 'cweid': '319', 'confidence': 'High', 'wascid': '15', 'description': 'HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.', 'messageId': '1777', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-319': 'https://cwe.mitre.org/data/definitions/319.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html\nhttps://owasp.org/www-community/Security_Headers\nhttps://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security\nhttps://caniuse.com/stricttransportsecurity\nhttps://datatracker.ietf.org/doc/html/rfc6797', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.', 'alert': 'Strict-Transport-Security Header Not Set', 'param': '', 'attack': '', 'name': 'Strict-Transport-Security Header Not Set', 'risk': 'Low', 'id': '9176', 'alertRef': '10035-1'}
{'sourceid': '3', '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.\nAt "High" threshold this scan rule will not alert on client or server error responses.', 'method': 'GET', 'evidence': '', 'pluginId': '10021', 'cweid': '693', 'confidence': 'Medium', 'wascid': '15', '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.", 'messageId': '1777',

'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'CWE-693': 'https://cwe.mitre.org/data/definitions/693.html', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html'}, 'reference': 'https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)\nhttps://owasp.org/www-community/Security_Headers', 'solution': "Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.\nIf 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.", 'alert': 'X-Content-Type-Options Header Missing', 'param': 'x-content-type-options', 'attack': '', 'name': 'X-Content-Type-Options Header Missing', 'risk': 'Low', 'id': '9184', 'alertRef': '10021'}

{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1777', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/jquery-2.1.1.min.js', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '9189', 'alertRef': '10037'}

{'sourceid': '3', 'other': 'CVE-2018-14041\nCVE-2019-8331\nCVE-2018-20677\nCVE-2018-20676\nCVE-2018-14042\nCVE-2016-10735\n', 'method': 'GET', 'evidence': '* Bootstrap v3.3.7', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium', 'wascid': '-1', 'description': 'The identified library bootstrap, version 3.3.7 is vulnerable.', 'messageId': '1773', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/js/bootstrap.min.js', 'tags': {'CVE-2018-14041': 'https://nvd.nist.gov/vuln/detail/CVE-2018-14041', 'CVE-2019-8331': 'https://nvd.nist.gov/vuln/detail/CVE-2019-8331', 'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.html', 'CVE-2018-20677': 'https://nvd.nist.gov/vuln/detail/CVE-2018-20677', 'CVE-2018-20676': 'https://nvd.nist.gov/vuln/detail/CVE-2018-20676', 'CVE-2018-14042': 'https://nvd.nist.gov/vuln/detail/CVE-2018-14042', 'CVE-2016-10735': 'https://nvd.nist.gov/vuln/detail/CVE-2016-10735', 'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/', 'CWE-829': 'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/twbs/bootstrap/issues/28236\nhttps://github.com/advisories/GHSA-pj7m-g53m-7638\nhttps://github.com/twbs/bootstrap/issues/20184\nhttps://github.com/advisories/GHSA-ph58-4vrj-w6hr\nhttps://github.com/twbs/bootstrap/issues/20631\nhttps://github.com/advisories/GHSA-4p24-vmcr-4gqj\nhttps://github.com/advisories/GHSA-9v3m-8fp8-mj99\nhttps://nvd.nist.gov/vuln/detail/CVE-2018-20676\n', 'solution': 'Please upgrade to the latest version of bootstrap.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk': 'Medium', 'id': '9191', 'alertRef': '10003'}

{'sourceid': '3', 'other': 'CVE-2020-11023\nCVE-2020-11022\nCVE-2015-9251\nCVE-2019-11358\n', 'method': 'GET', 'evidence': 'jquery-2.1.1.min.js', 'pluginId': '10003', 'cweid': '829', 'confidence': 'Medium',

```
'wascid': '-1', 'description': 'The identified library jquery, version 2.1.1 is vulnerable.', 'messageId': '1777',
'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/feedback/(S(vykpwigsozafja1fzjfhgvhh))/bootstrap/j
s/jquery-2.1.1.min.js', 'tags': {'CVE-2020-11023': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11023',
'OWASP_2017_A09': 'https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_
Known_Vulnerabilities.html', 'CVE-2020-11022': 'https://nvd.nist.gov/vuln/detail/CVE-2020-11022',
'OWASP_2021_A06': 'https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/',
'CVE-2015-9251': 'https://nvd.nist.gov/vuln/detail/CVE-2015-9251', 'CVE-2019-11358':
'https://nvd.nist.gov/vuln/detail/CVE-2019-11358', 'CWE-829':
'https://cwe.mitre.org/data/definitions/829.html'}, 'reference': 'https://github.com/jquery/jquery/issues/24
32\nhttp://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/\nhttp://research.insecurelabs.org/
jquery/test/\nhttps://blog.jquery.com/2019/04/10/jquery-3-4-0-released/\nhttps://nvd.nist.gov/vuln/detail/
CVE-2019-11358\nhttps://github.com/advisories/GHSA-rmxg-73gg-4p98\nhttps://nvd.nist.gov/vuln/deta
il/CVE-2015-9251\nhttps://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd08086
19b1b\nhttps://bugs.jquery.com/ticket/11974\nhttps://github.com/jquery/jquery.com/issues/162\nhttps://
blog.jquery.com/2020/04/10/jquery-3-5-0-released/\n', 'solution': 'Please upgrade to the latest version of
jquery.', 'alert': 'Vulnerable JS Library', 'param': '', 'attack': '', 'name': 'Vulnerable JS Library', 'risk':
'Medium', 'id': '9199', 'alertRef': '10003'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'POST', 'evidence':
'cbhqk1udfl33y2lkmebsut4i', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1836', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9480', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1844', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/AttWfForgotPass.aspx', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9508', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'alkty2mthqhzw5glqh0ztgb0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'Medium', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1843', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9534', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1847', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-1.7.1.intellisense.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9540', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1874', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9563', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'ovuxbzapnsn2ve5sl5emnqr2', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1849', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/play.png', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9572', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cbhqk1udfl33y2lkmebsut4i', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1875', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/_references.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9616', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'alkty2mthqhzw5glqh0ztgb0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1873', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/accounts.jpg', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
```

'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9618', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'alkty2mthqhzw5glqh0ztgb0', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1878', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/ScriptResource.axd
?d=nnHyWnZ5bTPuYszCeiYmKwzPD-Sda5c6unHER_wN3RYGsJdrp9mJsDTSMAlFEqmeMCa9PKx
UvgOctjh3nF3Yl4CcoSALp0ll-wH_9LUt9qxDJdA6Q-LhgyXzPJhLvZwK6TYZxreyb3iHfSauSm9l3oXsriY
gReyv3ohx7-ei-o01&t=10c151ff', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9628', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cbhqk1udfl33y2lkmebsut4i', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1877', 'inputVector': '', 'url':
'https://ecampus.psgtech.ac.in/studzone2/Scripts/jquery-ui-1.8.20.js', 'tags': {}, 'reference':
'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id', 'solution': 'This
is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert': 'Session
Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9642', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1879', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/favicon.ico', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9667', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'zh2frcg4h5kshxe3tv30wzrt', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1881', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/engine1/play.png', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9723', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cohtcorufno55p3lcppeaqg5', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',

```
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1888', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/studzone2/', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9805', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'mv3ubtxzx5xmagi2rvf3ru1t', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1907', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/psglogo.jpg', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9833', 'alertRef': '10112'}
{'sourceid': '3', 'other': '\ncookie:ASP.NET_SessionId', 'method': 'GET', 'evidence':
'cbhqk1udfl33y2lkmebsut4i', 'pluginId': '10112', 'cweid': '-1', 'confidence': 'High', 'wascid': '-1',
'description': 'The given response has been identified as containing a session management token. The
\'Other Info\' field contains a set of header tokens that can be used in the Header Based Session
Management Method. If the request is in a context which has a Session Management Method set to
"Auto-Detect" then this rule will change the session management to use the tokens identified.',
'messageId': '1906', 'inputVector': '', 'url': 'https://ecampus.psgtech.ac.in/Images/psglogo.jpg', 'tags': {},
'reference': 'https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id',
'solution': 'This is an informational alert rather than a vulnerability and so there is nothing to fix.', 'alert':
'Session Management Response Identified', 'param': 'ASP.NET_SessionId', 'attack': '', 'name': 'Session
Management Response Identified', 'risk': 'Informational', 'id': '9834', 'alertRef': '10112'}
Active Scanning target http://ecampus.psgtech.ac.in
Scan progress %: 7
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 12
Scan progress %: 39
Scan progress %: 39
Scan progress %: 39
Scan progress %: 39
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Scan progress %: 46
Active Scan completed
Hosts: ecampus.psgtech.ac.in, ecampus.psgtech.ac.in
Alerts:
```

```
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '1', 'inputVector': '', 'url': 'http://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': '', 'attack': '', 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '0', 'alertRef': '10036'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '1', 'inputVector': '', 'url': 'http://ecampus.psgtech.ac.in/', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)', 'risk': 'Low', 'id': '1', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '11', 'inputVector': '', 'url': 'http://ecampus.psgtech.ac.in/robots.txt', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200':
```

'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': ", 'attack': ", 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '12', 'alertRef': '10036'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '9', 'inputVector': ", 'url': 'http://ecampus.psgtech.ac.in', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': ", 'attack': ", 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '13', 'alertRef': '10036'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'Microsoft-IIS/8.0', 'pluginId': '10036', 'cweid': '200', 'confidence': 'High', 'wascid': '13', '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.', 'messageId': '13', 'inputVector': ", 'url': 'http://ecampus.psgtech.ac.in/sitemap.xml', 'tags': {'OWASP_2021_A05': 'https://owasp.org/Top10/A05_2021-Security_Misconfiguration/', 'OWASP_2017_A06': 'https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html', 'WSTG-v42-INFO-02': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://httpd.apache.org/docs/current/mod/core.html#servertokens\nhttps://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10)\nhttps://www.troyhunt.com/shhh-dont-let-your-response-headers/', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.', 'alert': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'param': ", 'attack': ", 'name': 'Server Leaks Version Information via "Server" HTTP Response Header Field', 'risk': 'Low', 'id': '14', 'alertRef': '10036'}
{'sourceid': '3', 'other': ", 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037', 'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '11', 'inputVector': ", 'url': 'http://ecampus.psgtech.ac.in/robots.txt', 'tags': {'OWASP_2021_A01': 'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03': 'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200': 'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to

```
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '17', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '13', 'inputVector': '', 'url':
'http://ecampus.psgtech.ac.in/sitemap.xml', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '18', 'alertRef': '10037'}
{'sourceid': '3', 'other': '', 'method': 'GET', 'evidence': 'X-Powered-By: ASP.NET', 'pluginId': '10037',
'cweid': '200', 'confidence': 'Medium', 'wascid': '13', '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.', 'messageId': '9', 'inputVector': '', 'url':
'http://ecampus.psgtech.ac.in', 'tags': {'OWASP_2021_A01':
'https://owasp.org/Top10/A01_2021-Broken_Access_Control/', 'WSTG-v42-INFO-08': 'https://owasp.or
g/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Ga
thering/08-Fingerprint_Web_Application_Framework', 'OWASP_2017_A03':
'https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.html', 'CWE-200':
'https://cwe.mitre.org/data/definitions/200.html'}, 'reference': 'https://owasp.org/www-project-web-securit
y-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_We
b_Application_Framework\nhttps://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.ht
ml', 'solution': 'Ensure that your web server, application server, load balancer, etc. is configured to
suppress "X-Powered-By" headers.', 'alert': 'Server Leaks Information via "X-Powered-By" HTTP
Response Header Field(s)', 'param': '', 'attack': '', 'name': 'Server Leaks Information via "X-Powered-By"
HTTP Response Header Field(s)', 'risk': 'Low', 'id': '19', 'alertRef': '10037'}
```

```
[+] Vulnerability Found: Server Leaks Version Information via "Server" HTTP Response Header Field
[+] Description: The web/application server is leaking version information via the "Server" HTTP
response header. Access to such information may facilitate attackers identifying other vulnerabilities
your web/application server is subject to.
[+] URL: http://ecampus.psgtech.ac.in/
[+] Vulnerability Found: 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://ecampus.psgtech.ac.in/
[+] Vulnerability Found: Server Leaks Version Information via "Server" HTTP Response Header Field
[+] Description: The web/application server is leaking version information via the "Server" HTTP
response header. Access to such information may facilitate attackers identifying other vulnerabilities
your web/application server is subject to.
[+] URL: http://ecampus.psgtech.ac.in/robots.txt
[+] Vulnerability Found: Server Leaks Version Information via "Server" HTTP Response Header Field
[+] Description: The web/application server is leaking version information via the "Server" HTTP
response header. Access to such information may facilitate attackers identifying other vulnerabilities
your web/application server is subject to.
[+] URL: http://ecampus.psgtech.ac.in
[+] Vulnerability Found: Server Leaks Version Information via "Server" HTTP Response Header Field
[+] Description: The web/application server is leaking version information via the "Server" HTTP
response header. Access to such information may facilitate attackers identifying other vulnerabilities
your web/application server is subject to.
[+] URL: http://ecampus.psgtech.ac.in/sitemap.xml
[+] Vulnerability Found: 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://ecampus.psgtech.ac.in/robots.txt
[+] Vulnerability Found: 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://ecampus.psgtech.ac.in/sitemap.xml
[+] Vulnerability Found: 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://ecampus.psgtech.ac.in
```