Website Security Scan Report

Generated on: 2024-12-11 19:03:55

Crawling Information

Crawled URL
http://vulnweb.com/acunetix-logo.png
http://vulnweb.com/sitemap.xml
http://vulnweb.com/robots.txt
http://vulnweb.com/

Scan Information

Target URL	http://vulnweb.com/	
Attack Type	All Attacks	
Scan Started At	2024-12-11 19:03:55	
Scan Duration	103.91 seconds	

Vulnerabilities Found

High Severity	0	
Medium Severity	936	
Low Severity	1417	

Vulnerability Details

URL	Risk	Description

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.

https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.

https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/report-anomaly-committee-2010	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Low	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	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.

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizens-charter-department-commerce	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	The page includes one or more script files from a third-party domain.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidance-booklet-marriages-overseas-indians	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/report-anomaly-committee-2010	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/report-anomaly-committee-2010	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A timestamp was disclosed by the application/web server. - Unix

https://www.india.gov.in/citizens-charter-department-commerce	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-commerce	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/guidelines-national-quality-monitors	Low	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
http://vulnweb.com/	Medium	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

http://vulnweb.com/sitemap.xml	Medium	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.
http://vulnweb.com/robots.txt	Medium	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.
http://vulnweb.com/acunetix-logo.png	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/acunetix-logo.png	Low	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.
http://vulnweb.com/sitemap.xml	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

http://vulnweb.com/robots.txt	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Medium	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.
http://vulnweb.com/	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/annual-report-reserve-bank-india	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/report-anomaly-committee-2010	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Low	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	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.

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizens-charter-department-commerce	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	The page includes one or more script files from a third-party domain.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/report-anomaly-committee-2010	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/report-anomaly-committee-2010	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A timestamp was disclosed by the application/web server. - Unix

https://www.india.gov.in/citizens-charter-department-commerce	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-commerce	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/guidelines-national-quality-monitors	Low	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
http://vulnweb.com/	Medium	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

http://vulnweb.com/sitemap.xml	Medium	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.
http://vulnweb.com/robots.txt	Medium	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.
http://vulnweb.com/acunetix-logo.png	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/acunetix-logo.png	Low	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.
http://vulnweb.com/sitemap.xml	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

http://vulnweb.com/robots.txt	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Medium	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.
http://vulnweb.com/	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/annual-report-reserve-bank-india	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/report-anomaly-committee-2010	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Low	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	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.

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizens-charter-department-commerce	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	The page includes one or more script files from a third-party domain.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidance-booklet-marriages-overseas-indians	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/report-anomaly-committee-2010	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/report-anomaly-committee-2010	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A timestamp was disclosed by the application/web server. - Unix

https://www.india.gov.in/citizens-charter-department-commerce	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-commerce	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/guidelines-national-quality-monitors	Low	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
http://vulnweb.com/	Medium	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

http://vulnweb.com/sitemap.xml	Medium	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.
http://vulnweb.com/robots.txt	Medium	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.
http://vulnweb.com/acunetix-logo.png	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/acunetix-logo.png	Low	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.
http://vulnweb.com/sitemap.xml	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

http://vulnweb.com/robots.txt	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Medium	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.
http://vulnweb.com/	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/annual-report-reserve-bank-india	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/report-anomaly-committee-2010	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Low	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	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.

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizens-charter-department-commerce	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	The page includes one or more script files from a third-party domain.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/report-anomaly-committee-2010	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/report-anomaly-committee-2010	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A timestamp was disclosed by the application/web server. - Unix

https://www.india.gov.in/citizens-charter-department-commerce	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-commerce	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/guidelines-national-quality-monitors	Low	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
http://vulnweb.com/	Medium	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

http://vulnweb.com/sitemap.xml	Medium	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.
http://vulnweb.com/robots.txt	Medium	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.
http://vulnweb.com/acunetix-logo.png	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/acunetix-logo.png	Low	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.
http://vulnweb.com/sitemap.xml	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

http://vulnweb.com/robots.txt	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Medium	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.
http://vulnweb.com/	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/annual-report-reserve-bank-india	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/report-anomaly-committee-2010	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Low	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	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.

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizens-charter-department-commerce	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	The page includes one or more script files from a third-party domain.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidance-booklet-marriages-overseas-indians	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/report-anomaly-committee-2010	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/report-anomaly-committee-2010	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A timestamp was disclosed by the application/web server. - Unix

https://www.india.gov.in/citizens-charter-department-commerce	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-commerce	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/guidelines-national-quality-monitors	Low	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
http://vulnweb.com/	Medium	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

http://vulnweb.com/sitemap.xml	Medium	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.
http://vulnweb.com/robots.txt	Medium	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.
http://vulnweb.com/acunetix-logo.png	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/acunetix-logo.png	Low	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.
http://vulnweb.com/sitemap.xml	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

http://vulnweb.com/robots.txt	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Medium	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.
http://vulnweb.com/	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/annual-report-reserve-bank-india	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/report-anomaly-committee-2010	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Low	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	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.

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizens-charter-department-commerce	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	The page includes one or more script files from a third-party domain.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/report-anomaly-committee-2010	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/report-anomaly-committee-2010	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A timestamp was disclosed by the application/web server. - Unix

https://www.india.gov.in/citizens-charter-department-commerce	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-commerce	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/guidelines-national-quality-monitors	Low	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
http://vulnweb.com/	Medium	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

http://vulnweb.com/sitemap.xml	Medium	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.
http://vulnweb.com/robots.txt	Medium	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.
http://vulnweb.com/acunetix-logo.png	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/acunetix-logo.png	Low	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.
http://vulnweb.com/sitemap.xml	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

http://vulnweb.com/robots.txt	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Medium	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.
http://vulnweb.com/	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/annual-report-reserve-bank-india	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/report-anomaly-committee-2010	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Low	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	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.

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizens-charter-department-commerce	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	The page includes one or more script files from a third-party domain.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/report-anomaly-committee-2010	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/report-anomaly-committee-2010	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A timestamp was disclosed by the application/web server. - Unix

https://www.india.gov.in/citizens-charter-department-commerce	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-commerce	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/guidelines-national-quality-monitors	Low	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
http://vulnweb.com/	Medium	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

http://vulnweb.com/sitemap.xml	Medium	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.
http://vulnweb.com/robots.txt	Medium	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.
http://vulnweb.com/acunetix-logo.png	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/acunetix-logo.png	Low	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.
http://vulnweb.com/sitemap.xml	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

http://vulnweb.com/robots.txt	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Medium	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.
http://vulnweb.com/	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/annual-report-reserve-bank-india	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/report-anomaly-committee-2010	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Low	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	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.

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizens-charter-department-commerce	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	The page includes one or more script files from a third-party domain.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/report-anomaly-committee-2010	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/report-anomaly-committee-2010	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A timestamp was disclosed by the application/web server. - Unix

https://www.india.gov.in/citizens-charter-department-commerce	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-commerce	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/guidelines-national-quality-monitors	Low	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
http://vulnweb.com/	Medium	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

http://vulnweb.com/sitemap.xml	Medium	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.
http://vulnweb.com/robots.txt	Medium	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.
http://vulnweb.com/acunetix-logo.png	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/acunetix-logo.png	Low	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.
http://vulnweb.com/sitemap.xml	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

http://vulnweb.com/robots.txt	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Medium	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.
http://vulnweb.com/	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/annual-report-reserve-bank-india	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/report-anomaly-committee-2010	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Low	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	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.

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizens-charter-department-commerce	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	The page includes one or more script files from a third-party domain.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/report-anomaly-committee-2010	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/report-anomaly-committee-2010	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A timestamp was disclosed by the application/web server. - Unix

https://www.india.gov.in/citizens-charter-department-commerce	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-commerce	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/guidelines-national-quality-monitors	Low	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
http://vulnweb.com/	Medium	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

http://vulnweb.com/sitemap.xml	Medium	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.
http://vulnweb.com/robots.txt	Medium	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.
http://vulnweb.com/acunetix-logo.png	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/acunetix-logo.png	Low	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.
http://vulnweb.com/sitemap.xml	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

http://vulnweb.com/robots.txt	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Medium	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.
http://vulnweb.com/	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/annual-report-reserve-bank-india	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/report-anomaly-committee-2010	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Low	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	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.

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizens-charter-department-commerce	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	The page includes one or more script files from a third-party domain.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/report-anomaly-committee-2010	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/report-anomaly-committee-2010	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A timestamp was disclosed by the application/web server. - Unix

https://www.india.gov.in/citizens-charter-department-commerce	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-commerce	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/guidelines-national-quality-monitors	Low	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
http://vulnweb.com/	Medium	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

http://vulnweb.com/sitemap.xml	Medium	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.
http://vulnweb.com/robots.txt	Medium	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.
http://vulnweb.com/acunetix-logo.png	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/acunetix-logo.png	Low	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.
http://vulnweb.com/sitemap.xml	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

http://vulnweb.com/robots.txt	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Medium	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.
http://vulnweb.com/	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/annual-report-reserve-bank-india	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/report-anomaly-committee-2010	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Low	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	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.

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizens-charter-department-commerce	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	The page includes one or more script files from a third-party domain.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidance-booklet-marriages-overseees-indians	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/report-anomaly-committee-2010	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/report-anomaly-committee-2010	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A timestamp was disclosed by the application/web server. - Unix

https://www.india.gov.in/citizens-charter-department-commerce	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-commerce	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/guidelines-national-quality-monitors	Low	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
http://vulnweb.com/	Medium	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

http://vulnweb.com/sitemap.xml	Medium	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.
http://vulnweb.com/robots.txt	Medium	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.
http://vulnweb.com/acunetix-logo.png	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/acunetix-logo.png	Low	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.
http://vulnweb.com/sitemap.xml	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

http://vulnweb.com/robots.txt	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Medium	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.
http://vulnweb.com/	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/annual-report-reserve-bank-india	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/report-anomaly-committee-2010	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Low	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	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.

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizens-charter-department-commerce	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	The page includes one or more script files from a third-party domain.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidance-booklet-marriages-overseas-indians	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/report-anomaly-committee-2010	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/report-anomaly-committee-2010	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A timestamp was disclosed by the application/web server. - Unix

https://www.india.gov.in/citizens-charter-department-commerce	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-commerce	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/guidelines-national-quality-monitors	Low	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
http://vulnweb.com/	Medium	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

http://vulnweb.com/sitemap.xml	Medium	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.
http://vulnweb.com/robots.txt	Medium	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.
http://vulnweb.com/acunetix-logo.png	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/acunetix-logo.png	Low	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.
http://vulnweb.com/sitemap.xml	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

http://vulnweb.com/robots.txt	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Medium	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.
http://vulnweb.com/	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/annual-report-reserve-bank-india	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.

https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/application-form-bsnl-broadband-service	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	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.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	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.

https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/report-anomaly-committee-2010	Low	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-commerce	Low	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.
https://www.india.gov.in/official-website-tourism-department-haryana	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/report-anomaly-committee-2010	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	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.

https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizens-charter-department-commerce	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/annual-report-reserve-bank-india	Informational	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.
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	The page includes one or more script files from a third-party domain.

https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.

https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Informational	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.
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Informational	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.
https://www.india.gov.in/guidelines-administrative-ministries-departments-and-public-sector-enterprises	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-haryana	Informational	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.
https://www.india.gov.in/annual-report-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.

https://www.india.gov.in/annual-report-reserve-bank-india	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Informational	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.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Informational	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.
https://www.india.gov.in/annual-report-reserve-bank-india	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.

https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Informational	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.
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Informational	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.
https://www.india.gov.in/report-anomaly-committee-2010	Informational	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.
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Informational	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.
https://www.india.gov.in/contact-details-nodal-officer-citizens-charter	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizen-charter-animal-husbandry-and-fisheries-chandigarh	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-commerce	Informational	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.
https://www.india.gov.in/citizen%E2%80%99s-charter-ministry-development-north-eastern-region	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/application-form-bsnl-broadband-service	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/official-website-tourism-department-haryana	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	X-Frame-Options (XFO) headers were found, a response with multiple XFO header entries may not be predictably treated by all user-agents.
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/report-anomaly-committee-2010	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).

https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidance-booklet-marriages-oversees-indians	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-maharashtra-tourism-development-corporation	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/report-anomaly-committee-2010	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/policies-and-guidelines-ministry-electronics-and-information-technology	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-applicants-service-quality-management-system	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/official-website-tourism-department-himachal-pradesh	Low	A timestamp was disclosed by the application/web server. - Unix

https://www.india.gov.in/citizens-charter-department-commerce	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/citizens-charter-department-commerce	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/citizens-charter-department-consumer-affairs	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.

https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Medium	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) 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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

https://www.india.gov.in/guidelines-national-quality-monitors	Low	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	The page includes one or more script files from a third-party domain.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Informational	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.
https://www.india.gov.in/guidelines-national-quality-monitors	Low	HTTP Strict Transport Security (HSTS) headers were found, a response with multiple HSTS header entries is not compliant with the specification (RFC 6797) and only the first HSTS header will be processed others will be ignored by user agents or the HSTS policy may be incorrectly applied. 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).
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
https://www.india.gov.in/guidelines-national-quality-monitors	Low	A timestamp was disclosed by the application/web server. - Unix
http://vulnweb.com/	Medium	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.

http://vulnweb.com/sitemap.xml	Medium	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.
http://vulnweb.com/robots.txt	Medium	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.
http://vulnweb.com/acunetix-logo.png	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/acunetix-logo.png	Low	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.
http://vulnweb.com/sitemap.xml	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

http://vulnweb.com/robots.txt	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Medium	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.
http://vulnweb.com/	Low	The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
http://vulnweb.com/	Low	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.