Nmap Scan Result

a. Summary - No. of Vulnerable Ports Open

Total Count : : **7**

b. Detailed Report

i. Port Number: 21

ii. Protocol: tcp

iii. Service: ftp

iv. Recommended Action or Best Practices: Ensure secure FTP configurations. Consider using SFTP or FTPS instead.

i. Port Number: 25

ii. Protocol: tcp

iii. Service: smtp

iv. Recommended Action or Best Practices: Implement proper email filtering and authentication mechanisms.

i. Port Number: 80

ii. Protocol: tcp

iii. Service: http

iv. Recommended Action or Best Practices: Apply security headers, keep software updated, and implement secure coding practices.

i. Port Number: 110

ii. Protocol: tcp

iii. Service: pop3

iv. Recommended Action or Best Practices: Consider using POP3 over SSL/TLS (POP3S) for secure email retrieval.

i. Port Number: 443

ii. Protocol: tcp

iii. Service: https

iv. Recommended Action or Best Practices: Apply security best practices for HTTPS services.

i. Port Number: 587

ii. Protocol: tcp

iii. Service: submission

iv. Recommended Action or Best Practices: Secure email submission by using submission over SSL/TLS.

i. Port Number: 993

ii. Protocol: tcp

iii. Service: imaps

iv. Recommended Action or Best Practices: Implement IMAPS (IMAP over SSL/TLS) for secure email access.

ZAP Scan Result

a. Summary

i. No. of Total Vulnerabilities Identified: : 698

ii. No. of Total Vulnerabilities Identified grouped on Risk Rating: : {'Medium': 98, 'Informational': 325, 'Low': 274, 'High': 1}

b. Detailed Report

i. Vulnerability Summary: Missing Anti-clickjacking Header

ii. Risk Rating: Medium

iii. Confidence Rating: Medium

iv. Description: The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** x-frame-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Missing Anti-clickjacking Header

ii. Risk Rating: Medium

iii. Confidence Rating: Medium

iv. Description: The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** x-frame-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Missing Anti-clickjacking Header

ii. Risk Rating: Medium

iii. Confidence Rating: Medium

iv. Description: The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** x-frame-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** no-store,no-cache,max-age=0

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** no-store,no-cache,max-age=0

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** no-store,no-cache,max-age=0

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Cookie No HttpOnly Flag

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: 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.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** nevercache-b39818
- **Attack:** No attack specified
- **Evidence:** Set-Cookie: nevercache-b39818

i. Vulnerability Summary: Cookie No HttpOnly Flag

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: 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.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** nevercache-b39818
- **Attack:** No attack specified
- **Evidence:** Set-Cookie: nevercache-b39818

i. Vulnerability Summary: Cookie No HttpOnly Flag

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: 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.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** nevercache-b39818
- **Attack:** No attack specified
- **Evidence:** Set-Cookie: nevercache-b39818

i. Vulnerability Summary: Cookie without SameSite Attribute

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** nevercache-b39818
- **Attack:** No attack specified
- **Evidence:** Set-Cookie: nevercache-b39818

i. Vulnerability Summary: Cookie without SameSite Attribute

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** nevercache-b39818
- **Attack:** No attack specified
- **Evidence:** Set-Cookie: nevercache-b39818

i. Vulnerability Summary: Cookie without SameSite Attribute

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** nevercache-b39818
- **Attack:** No attack specified
- **Evidence:** Set-Cookie: nevercache-b39818

i. Vulnerability Summary: Cookie Without Secure Flag

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** nevercache-b39818
- **Attack:** No attack specified
- **Evidence:** Set-Cookie: nevercache-b39818

i. Vulnerability Summary: Cookie Without Secure Flag

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** nevercache-b39818
- **Attack:** No attack specified
- **Evidence:** Set-Cookie: nevercache-b39818

i. Vulnerability Summary: Cookie Without Secure Flag

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** nevercache-b39818
- **Attack:** No attack specified
- **Evidence:** Set-Cookie: nevercache-b39818

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710734908

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710734908

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710734908

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Hidden File Found

ii. Risk Rating: Medium

iii. Confidence Rating: Low

iv. Description: A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/.hg
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** HTTP/1.1 202 Accepted

i. Vulnerability Summary: Hidden File Found

ii. Risk Rating: Medium

iii. Confidence Rating: Low

iv. Description: A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/.bzr
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** HTTP/1.1 202 Accepted

i. Vulnerability Summary: Hidden File Found

ii. Risk Rating: Medium

iii. Confidence Rating: Low

iv. Description: A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/._darcs
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** HTTP/1.1 202 Accepted

i. Vulnerability Summary: Hidden File Found

ii. Risk Rating: Medium

iii. Confidence Rating: Low

iv. Description: A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/BitKeeper
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** HTTP/1.1 202 Accepted

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** msnbot/1.1 (+http://search.msn.com/msnbot.htm)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
- **Evidence:** No evidence available

i. Vulnerability Summary: Missing Anti-clickjacking Header

ii. Risk Rating: Medium

iii. Confidence Rating: Medium

iv. Description: The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** x-frame-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** no-store,no-cache,max-age=0

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Cookie No HttpOnly Flag

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: 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.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** nevercache-b39818
- **Attack:** No attack specified
- **Evidence:** Set-Cookie: nevercache-b39818

i. Vulnerability Summary: Cookie without SameSite Attribute

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** nevercache-b39818
- **Attack:** No attack specified
- **Evidence:** Set-Cookie: nevercache-b39818

i. Vulnerability Summary: Cookie Without Secure Flag

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** nevercache-b39818
- **Attack:** No attack specified
- **Evidence:** Set-Cookie: nevercache-b39818

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710734935

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710734935

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710734935

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710734941

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt

- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710734941

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710734941

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** Header User-Agent

- **Attack:** Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)

- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** msnbot/1.1 (+http://search.msn.com/msnbot.htm)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** msnbot/1.1 (+http://search.msn.com/msnbot.htm)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** msnbot/1.1 (+http://search.msn.com/msnbot.htm)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** msnbot/1.1 (+http://search.msn.com/msnbot.htm)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
- **Evidence:** No evidence available

i. Vulnerability Summary: User Agent Fuzzer

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** Header User-Agent
- **Attack:** Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
- **Evidence:** No evidence available

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710735106

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710735106

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710735106

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml

- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710735122

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710735122

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710735122

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/infrastructure
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710735170

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710735170

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1710735170

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/even.pdf
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/robots.txt
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ac
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/sitemap.xml
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/NAAC22
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/career
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/captcha
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/NAAC22
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ac
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified

- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/even.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gallery
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/admission
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/career
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/Academicschedule/22/ACADEMIC_SCHEDULE.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/captcha
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Cross-Domain JavaScript Source File Inclusion

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The page includes one or more script files from a third-party domain.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/
- **Method:** GET
- **Parameter:** https://code.jquery.com/jquery-1.8.2.js
- **Attack:** No attack specified
- **Evidence:**

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/even.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gallery
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/admission
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/NAAC22
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/career
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ac
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/captcha
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/Academicschedule/22/ACADEMIC_SCHEDULE.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/even.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gallery
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/NAAC22
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Information Disclosure - Suspicious Comments

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

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

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/career
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** from

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ac
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Cookie No HttpOnly Flag

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: 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.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/captcha
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** Set-Cookie: csrftoken

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/admission
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/RulesandRegulations.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Information Disclosure - Suspicious Comments

ii. Risk Rating: Informational

iii. Confidence Rating: Low

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

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** user

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/even.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Cross-Domain JavaScript Source File Inclusion

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The page includes one or more script files from a third-party domain.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/captcha
- **Method:** GET
- **Parameter:** https://www.google.com/recaptcha/api.js
- **Attack:** No attack specified
- **Evidence:**

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gallery
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/robots.txt
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/NAAC22
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/career
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/sitemap.xml
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ac
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/admission
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/about
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/RulesandRegulations.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/secretarymessage
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Cross-Domain JavaScript Source File Inclusion

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The page includes one or more script files from a third-party domain.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/captcha
- **Method:** GET
- **Parameter:** https://maps.googleapis.com/maps/api/js?key=AIzaSyCcABaamniA6OL5YvYSpB3pFMNrXwXnLwU
- **Attack:** No attack specified
- **Evidence:**

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gallery
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/career
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/organisation_chart
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/iqac
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/admission
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/academic
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/governingbody
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/about
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/secretarymessage
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/captcha
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/docs/Institute%20Research%20Policy.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/organisation_chart
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/deanacademic
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified

- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/bosmeeting
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/iqac
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/academic
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/governingbody
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/principalmessage
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Cross-Domain JavaScript Source File Inclusion

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The page includes one or more script files from a third-party domain.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/about
- **Method:** GET
- **Parameter:** https://maps.googleapis.com/maps/api/js?key=AIzaSyCcABaamniA6OL5YvYSpB3pFMNrXwXnLwU
- **Attack:** No attack specified
- **Evidence:**

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/secretarymessage
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/13/27/

- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/captcha
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/deanacademic
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/bosmeeting
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/organisation_chart
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/iqac
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/principalmessage
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/governingbody
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/academic
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/captcha
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/secretarymessage
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/about
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/secretarymessage
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/about
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/organisation_chart
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/iqac
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/principalmessage
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/about
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/organisation_chart
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/governingbody
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/bosmeeting
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/iqac
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/principalmessage
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/academic
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/governingbody
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/bosmeeting
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/deanacademic
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/principalmessage
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/academic
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/bosmeeting
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/promotors
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/deanresearch
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/deanacademic
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/19/33
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/promotors
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/deanresearch
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/officebearers
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/20/34/
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/mb
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/deanacademic
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/endow
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/21/36
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/officebearers
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/mb
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/Ph.D.%20Guidelines.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/endow
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/promotors
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/deanresearch
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/officebearers
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/mb
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/endow
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/promotors
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/department
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/promotors
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/department
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/Ph.D.%20Guidelines.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Information Disclosure - Suspicious Comments

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

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

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/deanresearch
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** user

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/deanresearch
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/department
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/officebearers
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/deanresearch
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/officebearers
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/department
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/List%20of%20IPR%20events.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/mb
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/mb
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/programme
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/endow
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/List%20of%20Copyrights.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/department
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/endow
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/programme
- **Method:** GET
- **Parameter:** No parameter specified

- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/syllabus
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/syllabus
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/programme
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/aicte
- **Method:** GET

- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/programme
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/aicte
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/List-of-Patents_Website.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/28/44
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/programme
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/academicschedule
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/Revised%20Funded%20projects%20-%20KCET%20-16.07.2022.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/List%20of%20IPR%20events.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/aicte
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/29/45
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/academicschedule
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/about_research
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/about_research
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/regulations
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/aicte
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/syllabus
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/List%20of%20Copyrights.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rebio
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/List-of-Patents_Website.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/docs/Institute%20Research%20Policy.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/academicschedule
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rebio
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/31/47/
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/aicte
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/regulations
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/academicschedule
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/syllabus
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tab
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/about_research
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/Revised%20Funded%20projects%20-%20KCET%20-16.07.2022.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/academicschedule
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/syllabus
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tab
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Information Disclosure - Suspicious Comments

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

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

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/about_research
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** user

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/32/48
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/regulations
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rebio
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/advisory_board
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Information Disclosure - Suspicious Comments

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

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

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/about_research
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** from

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/advisory_board
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rebio
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/regulations
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rechem
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/about_research
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/33/49/
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rechem
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rebio
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/recse
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/regulations
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/33/49
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/about_research
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified

- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/advisory_board
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/recse
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/Revised%20Funded%20projects%20-%20KCET%20-16.07.2022.pdf
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rephy
- **Method:** GET
- **Parameter:** cache-control

- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/pool
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/34/50
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/reece
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Information Disclosure - Suspicious Comments

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

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

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/advisory_board
- **Method:** GET
- **Parameter:** No parameter specified

- **Attack:** No attack specified
- **Evidence:** user

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/Revised%20Funded%20projects%20-%20KCET%20-16.07.2022.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/recse
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rephy
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/gallery/thumnail
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/pool
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rechem
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/reece
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tab
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/advisory_board
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/reeee
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/Revised%20Funded%20projects%20-%20KCET%20-16.07.2022.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/37/53/
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rephy
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/reece
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/recse
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rechem
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/reeee
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/pool
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coe
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tab
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/advisory_board
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/Revised%20Funded%20projects%20-%20KCET%20-16.07.2022.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/exam_cell/R2017%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rechem
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rephy
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/recse
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/reece
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered

types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coe
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/reeee
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Information Disclosure - Suspicious Comments

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

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

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/pool
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** user

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/Revised%20Funded%20projects%20-%20KCET%20-16.07.2022.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tab
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/exam_cell/R2017%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/gallery/thumnail/DSC_5608.JPG
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/gallery/thumnail/DSC_5006.JPG
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/reece
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/rephy
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/ban/1.jpeg
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/reeee
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coe
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/pool
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/gallery/thumnail/DSC_3134.JPG
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/gallery/thumnail/DSC_1068.JPG
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/research_policy
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/recent
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/iqac_meetings/18th_IQAC_Meeting_Minutes.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/reece
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1615489138

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/members
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coe
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/pool
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/reeee
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/exam_cell/R2020%20PG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/iqac_meetings/12th_IQAC_Meeting_Minutes.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coecontact
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ipr
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/research_policy
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/recent
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Timestamp Disclosure - Unix

ii. Risk Rating: Low

iii. Confidence Rating: Low

iv. Description: A timestamp was disclosed by the application/web server - Unix

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/reece
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 1624489392

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/Amendment%20Notification%20Circular%20November%202023.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coe
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/members
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2017%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/exam_cell/R2020%20PG%20Timetable.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/minutes/FIFTH%20ACADEMIC%20COUNCIL%20MEETING%20MINUTES.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coecontact
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ipr
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/recent
- **Method:** GET
- **Parameter:** No parameter specified

- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/research_policy
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/boseng
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/Amendment%20Notification%20Circular%20November%202023.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/members
- **Method:** GET

- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2017%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coecirculars
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coecontact
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/Amendment%20Notification%20Circular%20November%202023.pdf

- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ipr
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/images/principal12.jfif
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Information Disclosure - Suspicious Comments

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

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

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/recent
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** user

i. Vulnerability Summary: Information Disclosure - Suspicious Comments

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

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

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/research_policy

- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** user

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/members
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2020%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2017%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coecirculars
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coecontact
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/Amendment%20Notification%20Circular%20November%202023.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/student_survey/BT_7.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Information Disclosure - Suspicious Comments

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

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

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ipr
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** user

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2021%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/exam_cell/SoP%20for%20applying%20for%20Transcript%20Certificate.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/recent
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/research_policy
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/members
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2017%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coecirculars
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered

types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2020%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coecontact
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/Amendment%20Notification%20Circular%20November%202023.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ipr
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2020%20PG%20Timetable.pdf
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2021%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/exam_cell/SoP%20for%20applying%20for%20Transcript%20Certificate.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/recent
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/research_policy
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2017%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coecirculars
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2020%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/Amendment%20Notification%20Circular%20November%202023.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ipr
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/AICTE/22/2006-2007.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2020%20PG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/student_survey/I_YEAR_PT.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2021%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Spring4Shell

ii. Risk Rating: High

iii. Confidence Rating: Medium

iv. Description: The application appears to be vulnerable to CVE-2022-22965 (otherwise known as Spring4Shell) - remote code execution (RCE) via data binding.

v. Details to Reproduce the Instance:

- **URL:** https://srcw.ac.in
- **Method:** POST
- **Parameter:** No parameter specified
- **Attack:** class.module.classLoader.DefaultAssertionStatus=nonsense
- **Evidence:** HTTP/1.1 400 Bad Request

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/minutes/REGULATION%20R2020.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/coecirculars
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2020%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/Amendment%20Notification%20Circular%20November%202023.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/department/banner/banner_chemistry_lEvsqWj.jpg
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Duplicate%20Semester%20Grade%20Sheet.pdf
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2020%20PG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/department/banner/DNS_9699.JPG
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2021%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/deptdetails/7
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/department/banner/banner_english_UwApgrb_4movUP4.jpg
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/exam_cell/SoP%20for%20applying%20for%20Duplicate%20Semester%20Grade%20Sheet.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20to%20Change%20the%20Name%20in%20Grade%20Sheets.pdf
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified

- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2020%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Transcript%20Certificate.pdf
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Duplicate%20Semester%20Grade%20Sheet.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/media/Revised%20Funded%20projects%20-%20KCET%20-16.07.2022.pdf

- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Scribe%20in%20End%20Semester%20Examinatinos.pdf
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2020%20PG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2021%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/images/pp2.jpg
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/exam_cell/SoP%20to%20Change%20the%20Name%20in%20Grade%20Sheets.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20to%20Change%20the%20Name%20in%20Grade%20Sheets.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/exam_cell/SoP%20for%20applying%20for%20Scribe%20in%20End%20Semester%20Examinatinos.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/exam_cell/SoP%20for%20applying%20for%20Duplicate%20Semester%20Grade%20Sheet.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Transcript%20Certificate.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/media/exam_cell/R2021%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Duplicate%20Semester%20Grade%20Sheet.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tdpc
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Scribe%20in%20End%20Semester%20Examinatinos.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/R2020%20PG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tdpteam
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/images/reee33.jpg
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20to%20Change%20the%20Name%20in%20Grade%20Sheets.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/exam_cell/SoP%20to%20Change%20the%20Name%20in%20Grade%20Sheets.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/exam_cell/SoP%20for%20applying%20for%20Scribe%20in%20End%20Semester%20Examinatinos.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/placement_drive/Slide12.JPG
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Transcript%20Certificate.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Duplicate%20Semester%20Grade%20Sheet.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tdpc
- **Method:** GET
- **Parameter:** No parameter specified

- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Scribe%20in%20End%20Semester%20Examinatinos.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/hostel/7.jpg
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tdpteam
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/p/datacenter/

- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/SM.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20to%20Change%20the%20Name%20in%20Grade%20Sheets.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ourrecruiters
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/cfe/AI1.jpg
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/cfe/1.jpg
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Transcript%20Certificate.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Duplicate%20Semester%20Grade%20Sheet.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tdpc
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Scribe%20in%20End%20Semester%20Examinatinos.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/library
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tdpteam
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered

types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/p/datacenter/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/SM.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20to%20Change%20the%20Name%20in%20Grade%20Sheets.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ourrecruiters
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/placementsrecords
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Transcript%20Certificate.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tdpc
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/timetable/'+deptID+'/media/exam_cell/SoP%20for%20applying%20for%20Scribe%20in%20End%20Semester%20Examinatinos.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/Faculty_Achievements/5
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/exam_cell/R2020%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/library
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tdpteam
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/p/datacenter/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/library/2
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/placementsrecords
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ourrecruiters
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified

- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/higher_studies/1/
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tdpc
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/NAAC22/NAAC%20DVV
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/value_added_courses/10/
- **Method:** GET

- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/placementcontact
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/exam_cell/R2020%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/library
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:**

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/tdpteam

- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/p/datacenter/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ourrecruiters
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/placementsrecords
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/edc
- **Method:** GET

- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/infra
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/iiic
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/studentprojectsts/7
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/placementcontact

- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/facilities
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/library
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/alumni_testimonials/7
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/p/datacenter/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/4/19/media/exam_cell/SoP%20to%20Change%20the%20Name%20in%20Grade%20Sheets.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/edc
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ourrecruiters
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/placementsrecords
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/infra
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/iiic
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/facilities
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/placementcontact
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/boys
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/girls
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/p/anti-ragging-committee/
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/hai/profile1
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/placementsrecords
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/edc
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/entrepreneur/5
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/infra
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/facilities
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/iiic
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/placementcontact
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/boys
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/girls
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/p/anti-ragging-committee/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/hai/profile1
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/NAAC22/AQAR/cr4/img/PG8.jpg
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/edc
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/co_curricular
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/infra
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/placementcontact
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/iiic
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/facilities
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/boys
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/girls
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/p/anti-ragging-committee/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/11/25/media/exam_cell/SoP%20to%20Change%20the%20Name%20in%20Grade%20Sheets.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/hai/profile1
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/extra_curricular
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/edc
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/co_curricular
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/infra
- **Method:** GET
- **Parameter:** No parameter specified

- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/iiic
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/facilities
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/boys
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/girls
- **Method:** GET

- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/p/anti-ragging-committee/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/gallery/images/DSC_0317.JPG
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/PLANNING%20AND%20MONITORING%20BOARD%20COMMITTEE.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Cookie No HttpOnly Flag

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: 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.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/hai/profile1

- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** Set-Cookie: csrftoken

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/extra_curricular
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/12/26/media/exam_cell
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/co_curricular
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/15/29/media/exam_cell/R2021%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/boys
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/gallery/images/DSC_3432.JPG
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/15/29/media/exam_cell/SoP%20for%20applying%20for%20Duplicate%20Semester%20Grade%20Sheet.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/girls
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/p/anti-ragging-committee/
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/PLANNING%20AND%20MONITORING%20BOARD%20COMMITTEE.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/STUDENT%20COUNSELLOR%20COMMITTEE.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Cross-Domain JavaScript Source File Inclusion

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The page includes one or more script files from a third-party domain.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/hai/profile1
- **Method:** GET
- **Parameter:** https://ajax.googleapis.com/ajax/libs/jquery/2.1.1/jquery.min.js
- **Attack:** No attack specified
- **Evidence:**

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/extra_curricular
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/FINANCE%20COMMITTEE%20MEMBERS.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/co_curricular
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/kcere
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/DISCIPLINE%20AND%20WELFARE%20COMMITTEE.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/26/42/media/Revised%20Funded%20projects%20-%20KCET%20-16.07.2022.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/SC%20ST%20COMMITTEE.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/25/41/media/exam_cell/R2021%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/gallery/images/DSC_6983.JPG
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/STUDENT%20COUNSELLOR%20COMMITTEE.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/25/41/media/exam_cell/SoP%20to%20Change%20the%20Name%20in%20Grade%20Sheets.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/hai/profile1
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:**

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/extra_curricular
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/FINANCE%20COMMITTEE%20MEMBERS.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/co_curricular
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/kcere
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/bootstrap/bootstrap.min.css
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/DISCIPLINE%20AND%20WELFARE%20COMMITTEE.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/slick/slick.css
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified

- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/SC%20ST%20COMMITTEE.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/aboutcfe
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/gallery/images/DSC_9753.JPG
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/do1.pdf
- **Method:** GET
- **Parameter:** No parameter specified

- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/hai/profile1
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/extra_curricular
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/40/56/media/exam_cell/R2021%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/gallery/images/DSC_2951.JPG

- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/kcere
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/bootstrap/bootstrap.min.css
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/gallery/images/DSC_2979.JPG
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/aboutcfe
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/slick/slick.css
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/gallery/images/DSC_4247.JPG
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ccna
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/do1.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/gallery/scripts/media/exam_cell/R2021%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/boss/bosad/1.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/animate-css/animate.css
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/slick/slick-theme.css
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/kcere
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/gal/45/61/media/TIME%20TABLE%20-%20I%20Sem%20Arrear%20Exam%20R2021.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/fontawesome/css/all.min.css
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/aboutcfe
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/css/style.css
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/department/staff/meenahod_9WJrCJA.jpg
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ccna
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/deptdetails/13/media/exam_cell/R2020%20PG%20Timetable.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Information Disclosure - Suspicious Comments

ii. Risk Rating: Informational

iii. Confidence Rating: Low

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

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/slick/slick.min.js
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** select

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/admiss_kcet
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/animate-css/animate.css
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/slick/slick-theme.css
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/kcere
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/Polymertech
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/fontawesome/css/all.min.css
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/aboutcfe
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/css/style.css
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/results
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ccna
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/human
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/slick/slick.min.js
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/admiss_kcet
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/club/11/media/exam_cell/R2020%20UG%20Timetable.pdf
- **Method:** GET
- **Parameter:** csrftoken

- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/infraimages/ct31_Y7vboXz.jpg
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/sscontent/3
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/Polymertech
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/aboutcfe
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/infraimages/ct35_95cjZKI.jpg
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/results
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/club/4/media/Amendment%20Notification%20Circular%20November%202023.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ccna
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/human
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/slick/slick.min.js
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/admiss_kcet
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/dailynews
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/honeywell
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/Smartant
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/Polymertech
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/innovit/2/media/exam_cell/SoP%20for%20applying%20for%20Scribe%20in%20End%20Semester%20Examinatinos.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/results
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Information Disclosure - Suspicious Comments

ii. Risk Rating: Informational

iii. Confidence Rating: Low

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

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/bootstrap/bootstrap.min.js
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** from

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/ccna
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/human
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/COMPLAINTS%20CUM%20REDRESSAL%20COMMITTEE.pdf
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/infraimages/ct74.jpg
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/admiss_kcet
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/dailynews
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/honeywell
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/Smartant
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/Polymertech
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/Tessolve
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/results
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/bootstrap/bootstrap.min.js
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Modern Web Application

ii. Risk Rating: Informational

iii. Confidence Rating: Medium

iv. Description: The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/human
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** Administration

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/images/f12.jpg
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/media/COMPLAINTS%20CUM%20REDRESSAL%20COMMITTEE.pdf
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/hebesec
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/admiss_kcet
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/dailynews
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/honeywell
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Private IP Disclosure

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: A private IP (such as 10.x.x.x, 172.x.x.x, 192.168.x.x) or an Amazon EC2 private hostname (for example, ip-10-0-56-78) has been found in the HTTP response body. This information might be helpful for further attacks targeting internal systems.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/Smartant
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** 10.10.20.4

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/Polymertech
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/results
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/Tessolve
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: X-Content-Type-Options Header Missing

ii. Risk Rating: Low

iii. Confidence Rating: Medium

iv. Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/plugins/bootstrap/bootstrap.min.js
- **Method:** GET
- **Parameter:** x-content-type-options
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Strict-Transport-Security Header Not Set

ii. Risk Rating: Low

iii. Confidence Rating: High

iv. Description: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/human
- **Method:** GET
- **Parameter:** No parameter specified

- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Re-examine Cache-control Directives

ii. Risk Rating: Informational

iii. Confidence Rating: Low

iv. Description: The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/nuvepro
- **Method:** GET
- **Parameter:** cache-control
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/vac/REVIT%20ARCHITECTURE.pdf
- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK

i. Vulnerability Summary: Content Security Policy (CSP) Header Not Set

ii. Risk Rating: Medium

iii. Confidence Rating: High

iv. Description: Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/hebesec
- **Method:** GET
- **Parameter:** No parameter specified
- **Attack:** No attack specified
- **Evidence:** No evidence available

i. Vulnerability Summary: Session Management Response Identified

ii. Risk Rating: Informational

iii. Confidence Rating: High

iv. Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.

v. Details to Reproduce the Instance:

- **URL:** https://kamarajengg.edu.in/static/vac/PRIMAVERA.pdf

- **Method:** GET
- **Parameter:** csrftoken
- **Attack:** No attack specified
- **Evidence:** N4NZhu1Thh17Kc1Odc9T1n0Ek0b5qifr5DPR49LcDlQO2WxniZsTiwOGqAxQDHCK