Vulnerabilities Report

1. Missing Anti-clickjacking Header

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

Tags:

OWASP_2021_A05

CWE-1021

SYSTEMIC

WSTG-v42-CLNT-09

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/

Method: GET

2. Application Error Disclosure

Description: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Tags:

WSTG-v42-ERRH-02

WSTG-v42-ERRH-01

OWASP_2021_A05

CWE-550

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/

Method: GET

3. Content Security Policy (CSP) Header Not Set

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/

Method: GET

4. Directory Browsing

Description: It is possible to view a listing of the directory contents. Directory listings may reveal hidden scripts, include files, backup source files, etc., which can be accessed to reveal sensitive information.

Tags:

OWASP_2021_A05

CWE-548

SYSTEMIC

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/

Method: GET

5. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/

Method: GET

6. X-Content-Type-Options Header Missing

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/

Method: GET

7. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

8. Missing Anti-clickjacking Header

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

Tags:

OWASP_2021_A05

CWE-1021

SYSTEMIC

WSTG-v42-CLNT-09

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=N;O=D

Method: GET

9. Application Error Disclosure

Description: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Tags:

WSTG-v42-ERRH-02

WSTG-v42-ERRH-01

OWASP_2021_A05

CWE-550

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=N;O=D

Method: GET

10. Content Security Policy (CSP) Header Not Set

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

ActiveX, audio and video files.

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=N;O=D

Method: GET

11. Directory Browsing

Description: It is possible to view a listing of the directory contents. Directory listings may reveal hidden scripts, include files, backup source files, etc., which can be accessed to reveal sensitive information.

Tags:

OWASP_2021_A05

CWE-548

SYSTEMIC

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=N;O=D

Method: GET

12. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=N;O=D

Method: GET

13. Missing Anti-clickjacking Header

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

Tags:

OWASP_2021_A05

CWE-1021

SYSTEMIC

WSTG-v42-CLNT-09

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=S;O=A

Method: GET

14. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute

Method: GET

15. X-Content-Type-Options Header Missing

Description: The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other

than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=N;O=D

Method: GET

16. Application Error Disclosure

Description: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Tags:

WSTG-v42-ERRH-02

WSTG-v42-ERRH-01

OWASP_2021_A05

CWE-550

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=S;O=A

Method: GET

17. Content Security Policy (CSP) Header Not Set

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=S;O=A

Method: GET

18. Directory Browsing

Description: It is possible to view a listing of the directory contents. Directory listings may reveal hidden scripts, include files, backup source files, etc., which can be accessed to reveal sensitive information.

Tags:

OWASP_2021_A05

CWE-548

SYSTEMIC

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=S;O=A

Method: GET

19. Missing Anti-clickjacking Header

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

Tags:

OWASP_2021_A05

CWE-1021

SYSTEMIC

WSTG-v42-CLNT-09

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=M;O=A

Method: GET

20. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=S;O=A

Method: GET

21. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

22. Application Error Disclosure

Description: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Tags:

WSTG-v42-ERRH-02

WSTG-v42-ERRH-01

OWASP_2021_A05

CWE-550

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=M;O=A

Method: GET

23. X-Content-Type-Options Header Missing

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=S;O=A

Method: GET

24. Content Security Policy (CSP) Header Not Set

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=M;O=A

Method: GET

25. Directory Browsing

Description: It is possible to view a listing of the directory contents. Directory listings may reveal hidden scripts, include files, backup source files, etc., which can be accessed to reveal sensitive information.

Tags:

OWASP_2021_A05

CWE-548

SYSTEMIC

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=M;O=A

Method: GET

26. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=M;O=A

Method: GET

27. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

28. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute

Method: GET

29. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

30. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Tags:

OWASP_2021_A01

WSTG-v42-INFO-08

SYSTEMIC

OWASP_2017_A03

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

31. X-Content-Type-Options Header Missing

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=M;O=A

Method: GET

32. Missing Anti-clickjacking Header

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

Tags:

OWASP_2021_A05

CWE-1021

SYSTEMIC

WSTG-v42-CLNT-09

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=D;O=A

Method: GET

33. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

34. Application Error Disclosure

Description: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Tags:

WSTG-v42-ERRH-02

WSTG-v42-ERRH-01

OWASP_2021_A05

CWE-550

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=D;O=A

Method: GET

35. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Tags:

OWASP_2021_A01

WSTG-v42-INFO-08

SYSTEMIC

OWASP_2017_A03

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

36. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

37. Content Security Policy (CSP) Header Not Set

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=D;O=A

Method: GET

38. Directory Browsing

Description: It is possible to view a listing of the directory contents. Directory listings may reveal hidden scripts, include files, backup source files, etc., which can be accessed to reveal sensitive information.

Tags:

OWASP_2021_A05

CWE-548

SYSTEMIC

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=D;O=A

Method: GET

39. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=D;O=A

Method: GET

40. X-Content-Type-Options Header Missing

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=D;O=A

Method: GET

41. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other

vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

42. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Tags:

OWASP_2021_A01

WSTG-v42-INFO-08

SYSTEMIC

OWASP_2017_A03

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

43. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/xss_r/

Method: GET

44. Missing Anti-clickjacking Header

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

Tags:

OWASP_2021_A05

CWE-1021

SYSTEMIC

WSTG-v42-CLNT-09

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=N;O=A

Method: GET

45. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

46. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Tags:

OWASP_2021_A01

WSTG-v42-INFO-08

SYSTEMIC

OWASP_2017_A03

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

47. Application Error Disclosure

Description: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Tags:

WSTG-v42-ERRH-02

WSTG-v42-ERRH-01

OWASP_2021_A05

CWE-550

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=N;O=A

Method: GET

48. Content Security Policy (CSP) Header Not Set

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=N;O=A

Method: GET

49. Directory Browsing

Description: It is possible to view a listing of the directory contents. Directory listings may reveal hidden scripts, include files, backup source files, etc., which can be accessed to reveal sensitive information.

Tags:

OWASP_2021_A05

CWE-548

SYSTEMIC

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=N;O=A

Method: GET

50. Directory Browsing

Description: It is possible to view a listing of the directory contents. Directory listings may reveal hidden scripts, include files, backup source files, etc., which can be accessed to reveal sensitive

information.

Tags:

OWASP_2021_A05

CWE-548

SYSTEMIC

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=S;O=D

Method: GET

51. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Tags:

OWASP_2021_A01

WSTG-v42-INFO-08

SYSTEMIC

OWASP_2017_A03

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/xss_r/

Method: GET

52. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=N;O=A

Method: GET

53. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/fi/

Method: GET

54. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Tags:

OWASP_2021_A01

WSTG-v42-INFO-08

SYSTEMIC

OWASP_2017_A03

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/fi/

Method: GET

55. X-Content-Type-Options Header Missing

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=N;O=A

Method: GET

56. Missing Anti-clickjacking Header

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

Tags:

OWASP_2021_A05

CWE-1021

SYSTEMIC

WSTG-v42-CLNT-09

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=M;O=D

Method: GET

57. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute

Method: GET

58. Missing Anti-clickjacking Header

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

Tags:

OWASP_2021_A05

CWE-1021

SYSTEMIC

WSTG-v42-CLNT-09

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=S;O=D

Method: GET

59. Application Error Disclosure

Description: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Tags:

WSTG-v42-ERRH-02

WSTG-v42-ERRH-01

OWASP_2021_A05

CWE-550

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=M;O=D

Method: GET

60. Application Error Disclosure

Description: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Tags:

WSTG-v42-ERRH-02

WSTG-v42-ERRH-01

OWASP_2021_A05

CWE-550

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=S;O=D

Method: GET

61. Content Security Policy (CSP) Header Not Set

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=M;O=D

Method: GET

62. Content Security Policy (CSP) Header Not Set

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=S;O=D

Method: GET

63. Directory Browsing

Description: It is possible to view a listing of the directory contents. Directory listings may reveal hidden scripts, include files, backup source files, etc., which can be accessed to reveal sensitive information.

Tags:

OWASP_2021_A05

CWE-548

SYSTEMIC

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=M;O=D

Method: GET

64. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute

Method: GET

65. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=M;O=D

Method: GET

66. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=S;O=D

Method: GET

67. X-Content-Type-Options Header Missing

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=M;O=D

Method: GET

68. X-Content-Type-Options Header Missing

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=S;O=D

Method: GET

69. Missing Anti-clickjacking Header

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

Tags:

OWASP_2021_A05

CWE-1021

SYSTEMIC

WSTG-v42-CLNT-09

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=D;O=D

Method: GET

70. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/upload/

Method: GET

71. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

72. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Tags:

OWASP_2021_A01

WSTG-v42-INFO-08

SYSTEMIC

OWASP_2017_A03

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/upload/

Method: GET

73. Application Error Disclosure

Description: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

Tags:

WSTG-v42-ERRH-02

WSTG-v42-ERRH-01

OWASP_2021_A05

CWE-550

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=D;O=D

Method: GET

74. Content Security Policy (CSP) Header Not Set

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=D;O=D

Method: GET

75. Directory Browsing

Description: It is possible to view a listing of the directory contents. Directory listings may reveal hidden scripts, include files, backup source files, etc., which can be accessed to reveal sensitive information.

Tags:

OWASP_2021_A05

CWE-548

SYSTEMIC

OWASP_2017_A06

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/?C=D;O=D

Method: GET

76. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/sqli/

Method: GET

77. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Tags:

OWASP_2021_A01

WSTG-v42-INFO-08

SYSTEMIC

OWASP_2017_A03

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/sqli/

Method: GET

78. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=D;O=D

Method: GET

79. X-Content-Type-Options Header Missing

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

Tags:

OWASP_2021_A05

SYSTEMIC

CWE-693

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/?C=D;O=D

Method: GET

80. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/sqli_blind/

Method: GET

81. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Tags:

OWASP_2021_A01

WSTG-v42-INFO-08

SYSTEMIC

OWASP_2017_A03

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/sqli_blind/

Method: GET

82. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/view_source_all.php

Method: GET

83. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Tags:

OWASP_2021_A01

WSTG-v42-INFO-08

SYSTEMIC

OWASP_2017_A03

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/view_source_all.php

Method: GET

84. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/view_help.php

Method: GET

85. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

86. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute

Method: GET

87. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Tags:

OWASP_2021_A01

WSTG-v42-INFO-08

SYSTEMIC

OWASP_2017_A03

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/view_help.php

Method: GET

88. Server Leaks Version Information via "Server" HTTP Response Header Field

Description: The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

Tags:

OWASP_2021_A05

SYSTEMIC

OWASP_2017_A06

WSTG-v42-INFO-02

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/view_source.php

Method: GET

89. Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description: The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

Tags:

OWASP_2021_A01

WSTG-v42-INFO-08

SYSTEMIC

OWASP_2017_A03

CWE-497

Risk: Low

URL: http://192.168.1.105/vulnerabilities/view_source.php

Method: GET

90. Cookie No HttpOnly Flag

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.

Tags:

CWE-1004

OWASP_2021_A05

WSTG-v42-SESS-02

SYSTEMIC

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

91. Cookie No HttpOnly Flag

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.

Tags:

CWE-1004

OWASP_2021_A05

WSTG-v42-SESS-02

SYSTEMIC

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

92. Cookie without SameSite Attribute

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.

Tags:

OWASP_2021_A01

WSTG-v42-SESS-02

SYSTEMIC

CWE-1275

OWASP_2017_A05

Risk: Low

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

93. Cookie without SameSite Attribute

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.

Tags:

OWASP_2021_A01

WSTG-v42-SESS-02

SYSTEMIC

CWE-1275

OWASP_2017_A05

Risk: Low

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

94. Cookie No HttpOnly Flag

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.

Tags:

CWE-1004

OWASP_2021_A05

WSTG-v42-SESS-02

SYSTEMIC

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

95. Cookie No HttpOnly Flag

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.

Tags:

CWE-1004

OWASP_2021_A05

WSTG-v42-SESS-02

SYSTEMIC

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

96. Cookie without SameSite Attribute

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.

Tags:

OWASP_2021_A01

WSTG-v42-SESS-02

SYSTEMIC

CWE-1275

OWASP_2017_A05

Risk: Low

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

97. Session Management Response Identified

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

Tags:

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

98. Cookie without SameSite Attribute

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.

Tags:

OWASP_2021_A01

WSTG-v42-SESS-02

SYSTEMIC

CWE-1275

OWASP_2017_A05

Risk: Low

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

99. Session Management Response Identified

Description: The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to

"Auto-Detect" then this rule will change the session management to use the tokens identified.

Tags:

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

100. Cookie No HttpOnly Flag

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.

Tags:

CWE-1004

OWASP_2021_A05

WSTG-v42-SESS-02

SYSTEMIC

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

101. Cookie without SameSite Attribute

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.

Tags:

OWASP_2021_A01

WSTG-v42-SESS-02

SYSTEMIC

CWE-1275

OWASP_2017_A05

Risk: Low

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

102. Cookie No HttpOnly Flag

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.

Tags:

CWE-1004

OWASP_2021_A05

WSTG-v42-SESS-02

SYSTEMIC

OWASP_2017_A06

Risk: Low

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

103. Cookie without SameSite Attribute

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.

Tags:

OWASP_2021_A01

WSTG-v42-SESS-02

SYSTEMIC

CWE-1275

OWASP_2017_A05

Risk: Low

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

104. Directory Browsing

Description: It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. which can be accessed to read sensitive information.

Tags:

OWASP_2021_A01

CWE-548

SYSTEMIC

OWASP_2017_A05

Risk: Medium

URL: http://192.168.1.105/vulnerabilities/

Method: GET

105. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute

Method: GET

106. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute

Method: GET

107. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute

Method: GET

108. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute

Method: GET

109. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

110. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

111. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute

Method: GET

112. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

113. User Agent Fuzzer

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

response body with the original response.

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute

Method: GET

114. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

115. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf

Method: GET

116. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute

Method: GET

117. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

118. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

119. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf

Method: GET

120. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

121. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

122. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

123. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf

Method: GET

124. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/brute/

Method: GET

125. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

126. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf

Method: GET

127. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

128. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf

Method: GET

129. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

130. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec

Method: GET

131. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf

Method: GET

132. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

133. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

134. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec

Method: GET

135. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

136. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf

Method: GET

137. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

138. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

139. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf

Method: GET

140. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec

Method: GET

141. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

142. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

143. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf

Method: GET

144. User Agent Fuzzer

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

response body with the original response.

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

145. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec

Method: GET

146. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

147. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

148. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf/

Method: GET

149. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf

Method: GET

150. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec

Method: GET

151. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

152. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf

Method: GET

153. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec

Method: GET

154. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

155. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/csrf

Method: GET

156. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec

Method: GET

157. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

158. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec

Method: GET

159. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

160. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec

Method: GET

161. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

162. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec/

Method: GET

163. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec

Method: GET

164. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi/

Method: GET

165. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi

Method: GET

166. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli

Method: GET

167. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi/

Method: GET

168. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec

Method: GET

169. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi

Method: GET

170. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/exec

Method: GET

171. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi/

Method: GET

172. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli

Method: GET

173. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi

Method: GET

174. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi/

Method: GET

175. User Agent Fuzzer

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

response body with the original response.

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi

Method: GET

176. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli

Method: GET

177. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi/

Method: GET

178. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi

Method: GET

179. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli

Method: GET

180. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi/

Method: GET

181. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli/

Method: GET

182. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli

Method: GET

183. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi/

Method: GET

184. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli/

Method: GET

185. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi

Method: GET

186. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi/

Method: GET

187. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli

Method: GET

188. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli/

Method: GET

189. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi

Method: GET

190. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi/

Method: GET

191. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli/

Method: GET

192. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli

Method: GET

193. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi

Method: GET

194. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli/

Method: GET

195. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi/

Method: GET

196. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli

Method: GET

197. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi

Method: GET

198. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli/

Method: GET

199. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi/

Method: GET

200. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli

Method: GET

201. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi

Method: GET

202. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli/

Method: GET

203. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi/

Method: GET

204. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli/

Method: GET

205. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli

Method: GET

206. User Agent Fuzzer

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

response body with the original response.

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi

Method: GET

207. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli/

Method: GET

208. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/fi

Method: GET

209. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli

Method: GET

210. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli/

Method: GET

211. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli

Method: GET

212. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli/

Method: GET

213. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli/

Method: GET

214. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload/

Method: GET

215. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload

Method: GET

216. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind/

Method: GET

217. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind

Method: GET

218. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload/

Method: GET

219. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind/

Method: GET

220. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload

Method: GET

221. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload/

Method: GET

222. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind

Method: GET

223. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload

Method: GET

224. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind/

Method: GET

225. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload/

Method: GET

226. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind/

Method: GET

227. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload/

Method: GET

228. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind

Method: GET

229. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload

Method: GET

230. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind/

Method: GET

231. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload/

Method: GET

232. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind

Method: GET

233. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload

Method: GET

234. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind/

Method: GET

235. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind

Method: GET

236. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload

Method: GET

237. User Agent Fuzzer

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

response body with the original response.

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind/

Method: GET

238. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload/

Method: GET

239. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind

Method: GET

240. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind/

Method: GET

241. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind

Method: GET

242. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload/

Method: GET

243. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind/

Method: GET

244. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload

Method: GET

245. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload/

Method: GET

246. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload/

Method: GET

247. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind

Method: GET

248. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind/

Method: GET

249. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload

Method: GET

250. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload

Method: GET

251. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload/

Method: GET

252. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind

Method: GET

253. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind/

Method: GET

254. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind/

Method: GET

255. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload

Method: GET

256. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload/

Method: GET

257. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind

Method: GET

258. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload

Method: GET

259. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind

Method: GET

260. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/upload

Method: GET

261. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/sqli_blind

Method: GET

262. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source.php

Method: GET

263. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r

Method: GET

264. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source_all.php

Method: GET

265. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_help.php

Method: GET

266. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source.php

Method: GET

267. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r

Method: GET

268. User Agent Fuzzer

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

response body with the original response.

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source.php

Method: GET

269. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_help.php

Method: GET

270. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source_all.php

Method: GET

271. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source_all.php

Method: GET

272. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r

Method: GET

273. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_help.php

Method: GET

274. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source.php

Method: GET

275. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source_all.php

Method: GET

276. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_help.php

Method: GET

277. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source.php

Method: GET

278. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r

Method: GET

279. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source.php

Method: GET

280. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_help.php

Method: GET

281. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source_all.php

Method: GET

282. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r

Method: GET

283. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source.php

Method: GET

284. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_help.php

Method: GET

285. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r

Method: GET

286. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source_all.php

Method: GET

287. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source.php

Method: GET

288. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_help.php

Method: GET

289. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source_all.php

Method: GET

290. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r

Method: GET

291. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source.php

Method: GET

292. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source_all.php

Method: GET

293. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_help.php

Method: GET

294. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r

Method: GET

295. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source.php

Method: GET

296. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_help.php

Method: GET

297. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source_all.php

Method: GET

298. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source.php

Method: GET

299. User Agent Fuzzer

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

response body with the original response.

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r

Method: GET

300. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_help.php

Method: GET

301. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source_all.php

Method: GET

302. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r

Method: GET

303. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source.php

Method: GET

304. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source_all.php

Method: GET

305. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_help.php

Method: GET

306. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r

Method: GET

307. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_source_all.php

Method: GET

308. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/view_help.php

Method: GET

309. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r

Method: GET

310. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r/

Method: GET

311. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

312. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r/

Method: GET

313. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s

Method: GET

314. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

315. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r/

Method: GET

316. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s

Method: GET

317. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r/

Method: GET

318. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

319. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

320. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s

Method: GET

321. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r/

Method: GET

322. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s

Method: GET

323. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

324. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r/

Method: GET

325. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

326. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s

Method: GET

327. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r/

Method: GET

328. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

329. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s

Method: GET

330. User Agent Fuzzer

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

response body with the original response.

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r/

Method: GET

331. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

332. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s

Method: GET

333. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r/

Method: GET

334. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

335. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s

Method: GET

336. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r/

Method: GET

337. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

338. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s

Method: GET

339. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r/

Method: GET

340. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s

Method: GET

341. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

342. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_r/

Method: GET

343. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s

Method: GET

344. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s/

Method: GET

345. User Agent Fuzzer

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

Tags:

SYSTEMIC

Risk: Informational

URL: http://192.168.1.105/vulnerabilities/xss_s

Method: GET