# Missing HTTP-Strict-Transport-Security-header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| MCS-BCK1 (10.2.10.6) | 5985 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing HTTP-Strict-Transport-Security-header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.\nHTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.\nCyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.Depending on the environment and the application this time period could be from as low as minutes to as long as days. | | | | |

# Missing Access-Control-Allow-Origin header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| MCS-BCK1 (10.2.10.6) | 5985 | TCP | LOW |  |
| TITLE | | | | |
| Missing Access-Control-Allow-Origin header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Forget about access control allow origin, here only to make script work, no hosts are affected. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| no solution needed | | | | |

# Missing X-Frame-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| MCS-BCK1 (10.2.10.6) | 5985 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Frame-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.\nThe server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.\nThe `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an `X-Frame-Options` header. | | | | |

# Missing Content-Security-Policy header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| MCS-BCK1 (10.2.10.6) | 5985 | TCP | LOW |  |
| TITLE | | | | |
| Missing Content-Security-Policy header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'. | | | | |

# Missing X-Content-Type-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| MCS-BCK1 (10.2.10.6) | 5985 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Content-Type-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.\nThe server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'. | | | | |

# Missing X-XSS-Protection header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| MCS-BCK1 (10.2.10.6) | 5985 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing X-XSS-Protection header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\nIf legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages. | | | | |

# Missing HTTP-Strict-Transport-Security-header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| MCS-BCK1 (10.2.10.6) | 5986 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing HTTP-Strict-Transport-Security-header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.\nHTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.\nCyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.Depending on the environment and the application this time period could be from as low as minutes to as long as days. | | | | |

# Missing Access-Control-Allow-Origin header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| MCS-BCK1 (10.2.10.6) | 5986 | TCP | LOW |  |
| TITLE | | | | |
| Missing Access-Control-Allow-Origin header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Forget about access control allow origin, here only to make script work, no hosts are affected. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| no solution needed | | | | |

# Missing X-Frame-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| MCS-BCK1 (10.2.10.6) | 5986 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Frame-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.\nThe server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.\nThe `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an `X-Frame-Options` header. | | | | |

# Missing Content-Security-Policy header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| MCS-BCK1 (10.2.10.6) | 5986 | TCP | LOW |  |
| TITLE | | | | |
| Missing Content-Security-Policy header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'. | | | | |

# Missing X-Content-Type-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| MCS-BCK1 (10.2.10.6) | 5986 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Content-Type-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.\nThe server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'. | | | | |

# Missing X-XSS-Protection header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| MCS-BCK1 (10.2.10.6) | 5986 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing X-XSS-Protection header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\nIf legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages. | | | | |

# Missing HTTP-Strict-Transport-Security-header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-VIRT-SRV2 (10.2.10.9) | 80 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing HTTP-Strict-Transport-Security-header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.\nHTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.\nCyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.Depending on the environment and the application this time period could be from as low as minutes to as long as days. | | | | |

# Missing Access-Control-Allow-Origin header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-VIRT-SRV2 (10.2.10.9) | 80 | TCP | LOW |  |
| TITLE | | | | |
| Missing Access-Control-Allow-Origin header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Forget about access control allow origin, here only to make script work, no hosts are affected. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| no solution needed | | | | |

# Missing X-Frame-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-VIRT-SRV2 (10.2.10.9) | 80 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Frame-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.\nThe server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.\nThe `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an `X-Frame-Options` header. | | | | |

# Missing Content-Security-Policy header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-VIRT-SRV2 (10.2.10.9) | 80 | TCP | LOW |  |
| TITLE | | | | |
| Missing Content-Security-Policy header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'. | | | | |

# Missing X-Content-Type-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-VIRT-SRV2 (10.2.10.9) | 80 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Content-Type-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.\nThe server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'. | | | | |

# Missing X-XSS-Protection header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-VIRT-SRV2 (10.2.10.9) | 80 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing X-XSS-Protection header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\nIf legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages. | | | | |

# Missing HTTP-Strict-Transport-Security-header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-VIRT-SRV2 (10.2.10.9) | 9080 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing HTTP-Strict-Transport-Security-header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.\nHTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.\nCyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.Depending on the environment and the application this time period could be from as low as minutes to as long as days. | | | | |

# Missing Access-Control-Allow-Origin header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-VIRT-SRV2 (10.2.10.9) | 9080 | TCP | LOW |  |
| TITLE | | | | |
| Missing Access-Control-Allow-Origin header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Forget about access control allow origin, here only to make script work, no hosts are affected. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| no solution needed | | | | |

# Missing Content-Security-Policy header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-VIRT-SRV2 (10.2.10.9) | 9080 | TCP | LOW |  |
| TITLE | | | | |
| Missing Content-Security-Policy header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'. | | | | |

# Missing X-Content-Type-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-VIRT-SRV2 (10.2.10.9) | 9080 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Content-Type-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.\nThe server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'. | | | | |

# Missing X-XSS-Protection header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-VIRT-SRV2 (10.2.10.9) | 9080 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing X-XSS-Protection header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\nIf legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages. | | | | |

# Missing HTTP-Strict-Transport-Security-header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.2.20.2) | 80 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing HTTP-Strict-Transport-Security-header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.\nHTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.\nCyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.Depending on the environment and the application this time period could be from as low as minutes to as long as days. | | | | |

# Missing Access-Control-Allow-Origin header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.2.20.2) | 80 | TCP | LOW |  |
| TITLE | | | | |
| Missing Access-Control-Allow-Origin header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Forget about access control allow origin, here only to make script work, no hosts are affected. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| no solution needed | | | | |

# Missing X-Frame-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.2.20.2) | 80 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Frame-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.\nThe server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.\nThe `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an `X-Frame-Options` header. | | | | |

# Missing Content-Security-Policy header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.2.20.2) | 80 | TCP | LOW |  |
| TITLE | | | | |
| Missing Content-Security-Policy header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'. | | | | |

# Missing X-Content-Type-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.2.20.2) | 80 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Content-Type-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.\nThe server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'. | | | | |

# Missing X-XSS-Protection header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.2.20.2) | 80 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing X-XSS-Protection header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\nIf legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages. | | | | |

# Missing HTTP-Strict-Transport-Security-header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.2.20.2) | 443 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing HTTP-Strict-Transport-Security-header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.\nHTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.\nCyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.Depending on the environment and the application this time period could be from as low as minutes to as long as days. | | | | |

# Missing Access-Control-Allow-Origin header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.2.20.2) | 443 | TCP | LOW |  |
| TITLE | | | | |
| Missing Access-Control-Allow-Origin header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Forget about access control allow origin, here only to make script work, no hosts are affected. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| no solution needed | | | | |

# Missing X-Frame-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.2.20.2) | 443 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Frame-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.\nThe server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.\nThe `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an `X-Frame-Options` header. | | | | |

# Missing Content-Security-Policy header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.2.20.2) | 443 | TCP | LOW |  |
| TITLE | | | | |
| Missing Content-Security-Policy header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'. | | | | |

# Missing X-Content-Type-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.2.20.2) | 443 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Content-Type-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.\nThe server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'. | | | | |

# Missing X-XSS-Protection header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.2.20.2) | 443 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing X-XSS-Protection header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\nIf legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages. | | | | |

# Missing HTTP-Strict-Transport-Security-header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.2.30.4) | 8080 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing HTTP-Strict-Transport-Security-header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.\nHTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.\nCyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.Depending on the environment and the application this time period could be from as low as minutes to as long as days. | | | | |

# Missing Access-Control-Allow-Origin header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.2.30.4) | 8080 | TCP | LOW |  |
| TITLE | | | | |
| Missing Access-Control-Allow-Origin header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Forget about access control allow origin, here only to make script work, no hosts are affected. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| no solution needed | | | | |

# Missing X-Frame-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.2.30.4) | 8080 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Frame-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.\nThe server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.\nThe `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an `X-Frame-Options` header. | | | | |

# Missing Content-Security-Policy header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.2.30.4) | 8080 | TCP | LOW |  |
| TITLE | | | | |
| Missing Content-Security-Policy header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'. | | | | |

# Missing X-Content-Type-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.2.30.4) | 8080 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Content-Type-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.\nThe server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'. | | | | |

# Missing X-XSS-Protection header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.2.30.4) | 8080 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing X-XSS-Protection header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\nIf legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages. | | | | |

# Missing HTTP-Strict-Transport-Security-header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.12.10.2) | 80 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing HTTP-Strict-Transport-Security-header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.\nHTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.\nCyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.Depending on the environment and the application this time period could be from as low as minutes to as long as days. | | | | |

# Missing Access-Control-Allow-Origin header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.12.10.2) | 80 | TCP | LOW |  |
| TITLE | | | | |
| Missing Access-Control-Allow-Origin header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Forget about access control allow origin, here only to make script work, no hosts are affected. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| no solution needed | | | | |

# Missing X-Frame-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.12.10.2) | 80 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Frame-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.\nThe server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.\nThe `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an `X-Frame-Options` header. | | | | |

# Missing Content-Security-Policy header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.12.10.2) | 80 | TCP | LOW |  |
| TITLE | | | | |
| Missing Content-Security-Policy header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'. | | | | |

# Missing X-Content-Type-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.12.10.2) | 80 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Content-Type-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.\nThe server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'. | | | | |

# Missing X-XSS-Protection header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.12.10.2) | 80 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing X-XSS-Protection header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\nIf legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages. | | | | |

# Missing HTTP-Strict-Transport-Security-header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.12.10.2) | 443 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing HTTP-Strict-Transport-Security-header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.\nHTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.\nCyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.Depending on the environment and the application this time period could be from as low as minutes to as long as days. | | | | |

# Missing Access-Control-Allow-Origin header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.12.10.2) | 443 | TCP | LOW |  |
| TITLE | | | | |
| Missing Access-Control-Allow-Origin header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Forget about access control allow origin, here only to make script work, no hosts are affected. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| no solution needed | | | | |

# Missing X-Frame-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.12.10.2) | 443 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Frame-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.\nThe server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.\nThe `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an `X-Frame-Options` header. | | | | |

# Missing Content-Security-Policy header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.12.10.2) | 443 | TCP | LOW |  |
| TITLE | | | | |
| Missing Content-Security-Policy header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'. | | | | |

# Missing X-Content-Type-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.12.10.2) | 443 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Content-Type-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.\nThe server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'. | | | | |

# Missing X-XSS-Protection header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-WAFW2 (10.12.10.2) | 443 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing X-XSS-Protection header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\nIf legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages. | | | | |

# Missing HTTP-Strict-Transport-Security-header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8080 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing HTTP-Strict-Transport-Security-header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.\nHTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.\nCyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.Depending on the environment and the application this time period could be from as low as minutes to as long as days. | | | | |

# Missing Access-Control-Allow-Origin header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8080 | TCP | LOW |  |
| TITLE | | | | |
| Missing Access-Control-Allow-Origin header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Forget about access control allow origin, here only to make script work, no hosts are affected. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| no solution needed | | | | |

# Missing X-Frame-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8080 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Frame-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.\nThe server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.\nThe `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an `X-Frame-Options` header. | | | | |

# Missing Content-Security-Policy header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8080 | TCP | LOW |  |
| TITLE | | | | |
| Missing Content-Security-Policy header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'. | | | | |

# Missing X-Content-Type-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8080 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Content-Type-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.\nThe server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'. | | | | |

# Missing X-XSS-Protection header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8080 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing X-XSS-Protection header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\nIf legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages. | | | | |

# Missing HTTP-Strict-Transport-Security-header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8081 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing HTTP-Strict-Transport-Security-header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.\nHTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.\nCyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.Depending on the environment and the application this time period could be from as low as minutes to as long as days. | | | | |

# Missing Access-Control-Allow-Origin header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8081 | TCP | LOW |  |
| TITLE | | | | |
| Missing Access-Control-Allow-Origin header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Forget about access control allow origin, here only to make script work, no hosts are affected. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| no solution needed | | | | |

# Missing X-Frame-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8081 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Frame-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.\nThe server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.\nThe `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an `X-Frame-Options` header. | | | | |

# Missing Content-Security-Policy header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8081 | TCP | LOW |  |
| TITLE | | | | |
| Missing Content-Security-Policy header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'. | | | | |

# Missing X-Content-Type-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8081 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Content-Type-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.\nThe server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'. | | | | |

# Missing X-XSS-Protection header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8081 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing X-XSS-Protection header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\nIf legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages. | | | | |

# Missing HTTP-Strict-Transport-Security-header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8090 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing HTTP-Strict-Transport-Security-header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.\nHTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.\nCyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.Depending on the environment and the application this time period could be from as low as minutes to as long as days. | | | | |

# Missing Access-Control-Allow-Origin header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8090 | TCP | LOW |  |
| TITLE | | | | |
| Missing Access-Control-Allow-Origin header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Forget about access control allow origin, here only to make script work, no hosts are affected. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| no solution needed | | | | |

# Missing X-Frame-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8090 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Frame-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.\nThe server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.\nThe `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an `X-Frame-Options` header. | | | | |

# Missing Content-Security-Policy header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8090 | TCP | LOW |  |
| TITLE | | | | |
| Missing Content-Security-Policy header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'. | | | | |

# Missing X-Content-Type-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8090 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Content-Type-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.\nThe server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'. | | | | |

# Missing X-XSS-Protection header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8090 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing X-XSS-Protection header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\nIf legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages. | | | | |

# Missing HTTP-Strict-Transport-Security-header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8091 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing HTTP-Strict-Transport-Security-header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.\nHTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.\nCyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.Depending on the environment and the application this time period could be from as low as minutes to as long as days. | | | | |

# Missing Access-Control-Allow-Origin header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8091 | TCP | LOW |  |
| TITLE | | | | |
| Missing Access-Control-Allow-Origin header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Forget about access control allow origin, here only to make script work, no hosts are affected. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| no solution needed | | | | |

# Missing X-Frame-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8091 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Frame-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.\nThe server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.\nThe `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an `X-Frame-Options` header. | | | | |

# Missing Content-Security-Policy header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8091 | TCP | LOW |  |
| TITLE | | | | |
| Missing Content-Security-Policy header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'. | | | | |

# Missing X-Content-Type-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8091 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Content-Type-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.\nThe server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'. | | | | |

# Missing X-XSS-Protection header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8091 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing X-XSS-Protection header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\nIf legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages. | | | | |

# Missing HTTP-Strict-Transport-Security-header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8442 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing HTTP-Strict-Transport-Security-header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP protocol by itself is clear text, meaning that any data that is transmitted via HTTP can be captured and the contents viewed. To keep data private and prevent it from being intercepted, HTTP is often tunnelled through either Secure Sockets Layer (SSL) or Transport Layer Security (TLS). When either of these encryption standards are used, it is referred to as HTTPS.\nHTTP Strict Transport Security (HSTS) is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. This will be enforced by the browser even if the user requests a HTTP resource on the same server.\nCyber-criminals will often attempt to compromise sensitive information passed from the client to the server using HTTP. This can be conducted via various Man-in-The-Middle (MiTM) attacks or through network packet captures. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Depending on the framework being used the implementation methods will vary, however it is advised that the `Strict-Transport-Security` header be configured on the server.One of the options for this header is `max-age`, which is a representation (in milliseconds) determining the time in which the client's browser will adhere to the header policy.Depending on the environment and the application this time period could be from as low as minutes to as long as days. | | | | |

# Missing Access-Control-Allow-Origin header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8442 | TCP | LOW |  |
| TITLE | | | | |
| Missing Access-Control-Allow-Origin header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Forget about access control allow origin, here only to make script work, no hosts are affected. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| no solution needed | | | | |

# Missing X-Frame-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8442 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Frame-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.\nThe server didn't return an `X-Frame-Options` header which means that this website could be at risk of a clickjacking attack.\nThe `X-Frame-Options` HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an `X-Frame-Options` header. | | | | |

# Missing Content-Security-Policy header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8442 | TCP | LOW |  |
| TITLE | | | | |
| Missing Content-Security-Policy header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| Content Security Policy (CSP) is a web security standard that helps to mitigate attacks like cross-site scripting (XSS), clickjacking or mixed content issues. CSP provides mechanisms to websites to restrict content that browsers will be allowed to load. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure Content Security Policy on your website by adding 'Content-Security-Policy' HTTP header or meta tag http-equiv='Content-Security-Policy'. | | | | |

# Missing X-Content-Type-Options header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8442 | TCP | LOW |  |
| TITLE | | | | |
| Missing X-Content-Type-Options header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-Content-Type-Options' response header prevents the browser from MIME-sniffing a response away from the declared content-type.\nThe server did not return a correct 'X-Content-Type-Options' header, which means that this website could be at risk of a Cross-Site Scripting (XSS) attack. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-Content-Type-Options' header with a value of 'nosniff'. | | | | |

# Missing X-XSS-Protection header

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| HOST | PORT | PROTOCOL | SEVERITY | CODE |
| GDAP-Helpdesk (10.12.30.4) | 8442 | TCP | MEDIUM |  |
| TITLE | | | | |
| Missing X-XSS-Protection header | | | | |
| STATE | | | | |
| **OPEN** | | | | |
| CVSS 3.1 | | | | |
| CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N | | | | |
| DESCRIPTION | | | | |
| The HTTP 'X-XSS-Protection' response header is a feature of modern browsers that allows websites to control their XSS auditors.\nThe server is not configured to return a 'X-XSS-Protection' header which means that any pages on this website could be at risk of a Cross-Site Scripting (XSS) attack. This URL is flagged as a specific example.\nIf legacy browsers support is not needed, it is recommended to use Content-Security-Policy without allowing unsafe-inline scripts instead. | | | | |
| EVIDENCE | | | | |
| Figure 5 – Evidence | | | | |
| SOLUTION | | | | |
| Configure your web server to include an 'X-XSS-Protection' header with a value of '1; mode=block' on all pages. | | | | |