C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

Cleartext Password over HTTP

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Environment**](about:blank#description) |
| **Resource** | **/** |
| **Risk** | **High** |

**Request**

[**GET /**](about:blank)

**Discussion**

Vega detected a form with a password input field that submits to an insecure (HTTP) target. Password values should never be sent in the clear across insecure channels. This vulnerability could result in unauthorized disclosure of passwords to passive network attackers.

**Impact**

* Vega has detected a form that can cause a password submission over an insecure channel.
* This could result in disclosure of passwords to network eavesdroppers.

**Remediation**

* Passwords should never be sent over cleartext. The form should submit to an HTTPS target.

**References**

Some additional links with relevant information published by third-parties:

* [**HTTPS (Wikipedia)**](http://en.wikipedia.org/wiki/HTTP_Secure)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

ASP/ASPX Error Detected

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/Errors** |
| **Risk** | Low |

**Request**

[**GET /Errors?aspxerrorpath=/Scripts/msdn.microsoft.com/en-us/%0A%20-->">'>'"**](about:blank)

**Resource Content**

|  |
| --- |
| <span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1> |

**Discussion**

Vega has detected an error message associated with the Microsoft ASP/ASP.NET framework.

**Impact**

* Verbose error output has been detected.
* Data in this output could reveal sensitive information about the application that could aid more complex attacks.
* The error itself may be indicative of a security vulnerability.

**Remediation**

* The developer should investigate the error to determine its nature and ensure that it does not represent a vulnerability.
* Disable error messages for remote users.
* Configure the server and framework to display safe error messages that do not include sensitive information.

**References**

Some additional links with relevant information published by third-parties:

* [**MSDN - How to: Display Safe Error Messages**](http://msdn.microsoft.com/en-us/library/994a1482(v=vs.100).aspx)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

ASP/ASPX Error Detected

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/Errors/** |
| **Risk** | Low |

**Request**

[**GET /Errors/?aspxerrorpath=/Scripts/msdn.microsoft.com/en-us/**](about:blank)

**Resource Content**

|  |
| --- |
| <span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1> |

**Discussion**

Vega has detected an error message associated with the Microsoft ASP/ASP.NET framework.

**Impact**

* Verbose error output has been detected.
* Data in this output could reveal sensitive information about the application that could aid more complex attacks.
* The error itself may be indicative of a security vulnerability.

**Remediation**

* The developer should investigate the error to determine its nature and ensure that it does not represent a vulnerability.
* Disable error messages for remote users.
* Configure the server and framework to display safe error messages that do not include sensitive information.

**References**

Some additional links with relevant information published by third-parties:

* [**MSDN - How to: Display Safe Error Messages**](http://msdn.microsoft.com/en-us/library/994a1482(v=vs.100).aspx)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

Character Set Not Specified

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/Content/** |
| **Risk** | Info |

**Request**

[**GET /Content/**](about:blank)

**Resource Content**

|  |
| --- |
| /Content/ |

**Discussion**

Vega has detected that the resource has not specified a character set in the response. If the character set is not specified, the browser may make assumptions about the character set based on resource content. This may present a security concern if the affected resource contains dynamically-generated content that originates from users. In such a case, malicious users may potentially take advantage of how specific browsers interpret characters to cause malicious content to be rendered. For example, an attacker may be able to bypass a cross-site scripting filter by encoding their malicious payload in an alternate character set, which may be executed depending on how the browser interprets the encoded content.

**Remediation**

* Specify a well-defined character set (such as UTF-8) within the response header content-type or the response body.

**References**

Some additional links with relevant information published by third-parties:

* [**OWASP Top Ten Cheat Sheet**](https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

Character Set Not Specified

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/Errors/NotFound** |
| **Risk** | Info |

**Request**

[**GET /Errors/NotFound?aspxerrorpath=/Scripts/msdn.microsoft.com/en-us/'%20-->">'>'"**](about:blank)

**Resource Content**

|  |
| --- |
| /Errors/NotFound?aspxerrorpath=/Scripts/msdn.microsoft.com/en-us/'%20-->">'>'"<vvv000127v218727> |

**Discussion**

Vega has detected that the resource has not specified a character set in the response. If the character set is not specified, the browser may make assumptions about the character set based on resource content. This may present a security concern if the affected resource contains dynamically-generated content that originates from users. In such a case, malicious users may potentially take advantage of how specific browsers interpret characters to cause malicious content to be rendered. For example, an attacker may be able to bypass a cross-site scripting filter by encoding their malicious payload in an alternate character set, which may be executed depending on how the browser interprets the encoded content.

**Remediation**

* Specify a well-defined character set (such as UTF-8) within the response header content-type or the response body.

**References**

Some additional links with relevant information published by third-parties:

* [**OWASP Top Ten Cheat Sheet**](https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

Character Set Not Specified

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/Scripts/** |
| **Risk** | Info |

**Request**

[**GET /Scripts/**](about:blank)

**Resource Content**

|  |
| --- |
| /Scripts/ |

**Discussion**

Vega has detected that the resource has not specified a character set in the response. If the character set is not specified, the browser may make assumptions about the character set based on resource content. This may present a security concern if the affected resource contains dynamically-generated content that originates from users. In such a case, malicious users may potentially take advantage of how specific browsers interpret characters to cause malicious content to be rendered. For example, an attacker may be able to bypass a cross-site scripting filter by encoding their malicious payload in an alternate character set, which may be executed depending on how the browser interprets the encoded content.

**Remediation**

* Specify a well-defined character set (such as UTF-8) within the response header content-type or the response body.

**References**

Some additional links with relevant information published by third-parties:

* [**OWASP Top Ten Cheat Sheet**](https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

Character Set Not Specified

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/Scripts/.enctype%2Ct.html5Clone%3D** |
| **Risk** | Info |

**Request**

[**GET /Scripts/.enctype%2Ct.html5Clone%3D**](about:blank)

**Resource Content**

|  |
| --- |
| /Scripts/.enctype%2Ct.html5Clone%3D |

**Discussion**

Vega has detected that the resource has not specified a character set in the response. If the character set is not specified, the browser may make assumptions about the character set based on resource content. This may present a security concern if the affected resource contains dynamically-generated content that originates from users. In such a case, malicious users may potentially take advantage of how specific browsers interpret characters to cause malicious content to be rendered. For example, an attacker may be able to bypass a cross-site scripting filter by encoding their malicious payload in an alternate character set, which may be executed depending on how the browser interprets the encoded content.

**Remediation**

* Specify a well-defined character set (such as UTF-8) within the response header content-type or the response body.

**References**

Some additional links with relevant information published by third-parties:

* [**OWASP Top Ten Cheat Sheet**](https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

Character Set Not Specified

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/Scripts/.html(** |
| **Risk** | Info |

**Request**

[**GET /Scripts/.html(**](about:blank)

**Resource Content**

|  |
| --- |
| /Scripts/.html( |

**Discussion**

Vega has detected that the resource has not specified a character set in the response. If the character set is not specified, the browser may make assumptions about the character set based on resource content. This may present a security concern if the affected resource contains dynamically-generated content that originates from users. In such a case, malicious users may potentially take advantage of how specific browsers interpret characters to cause malicious content to be rendered. For example, an attacker may be able to bypass a cross-site scripting filter by encoding their malicious payload in an alternate character set, which may be executed depending on how the browser interprets the encoded content.

**Remediation**

* Specify a well-defined character set (such as UTF-8) within the response header content-type or the response body.

**References**

Some additional links with relevant information published by third-parties:

* [**OWASP Top Ten Cheat Sheet**](https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

Character Set Not Specified

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/Scripts/.html(this.message** |
| **Risk** | Info |

**Request**

[**GET /Scripts/.html(this.message**](about:blank)

**Resource Content**

|  |
| --- |
| /Scripts/.html(this.message |

**Discussion**

Vega has detected that the resource has not specified a character set in the response. If the character set is not specified, the browser may make assumptions about the character set based on resource content. This may present a security concern if the affected resource contains dynamically-generated content that originates from users. In such a case, malicious users may potentially take advantage of how specific browsers interpret characters to cause malicious content to be rendered. For example, an attacker may be able to bypass a cross-site scripting filter by encoding their malicious payload in an alternate character set, which may be executed depending on how the browser interprets the encoded content.

**Remediation**

* Specify a well-defined character set (such as UTF-8) within the response header content-type or the response body.

**References**

Some additional links with relevant information published by third-parties:

* [**OWASP Top Ten Cheat Sheet**](https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

Character Set Not Specified

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/Scripts/.length%2Ct.htmlSerialize%3D%21%21d.getElementsByTagName(** |
| **Risk** | Info |

**Request**

[**GET /Scripts/.length%2Ct.htmlSerialize%3D%21%21d.getElementsByTagName(**](about:blank)

**Resource Content**

|  |
| --- |
| /Scripts/.length%2Ct.htmlSerialize%3D%21%21d.getElementsByTagName( |

**Discussion**

Vega has detected that the resource has not specified a character set in the response. If the character set is not specified, the browser may make assumptions about the character set based on resource content. This may present a security concern if the affected resource contains dynamically-generated content that originates from users. In such a case, malicious users may potentially take advantage of how specific browsers interpret characters to cause malicious content to be rendered. For example, an attacker may be able to bypass a cross-site scripting filter by encoding their malicious payload in an alternate character set, which may be executed depending on how the browser interprets the encoded content.

**Remediation**

* Specify a well-defined character set (such as UTF-8) within the response header content-type or the response body.

**References**

Some additional links with relevant information published by third-parties:

* [**OWASP Top Ten Cheat Sheet**](https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

Character Set Not Specified

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/Scripts/%2Cs.html(i** |
| **Risk** | Info |

**Request**

[**GET /Scripts/%2Cs.html(i**](about:blank)

**Resource Content**

|  |
| --- |
| /Scripts/%2Cs.html(i |

**Discussion**

Vega has detected that the resource has not specified a character set in the response. If the character set is not specified, the browser may make assumptions about the character set based on resource content. This may present a security concern if the affected resource contains dynamically-generated content that originates from users. In such a case, malicious users may potentially take advantage of how specific browsers interpret characters to cause malicious content to be rendered. For example, an attacker may be able to bypass a cross-site scripting filter by encoding their malicious payload in an alternate character set, which may be executed depending on how the browser interprets the encoded content.

**Remediation**

* Specify a well-defined character set (such as UTF-8) within the response header content-type or the response body.

**References**

Some additional links with relevant information published by third-parties:

* [**OWASP Top Ten Cheat Sheet**](https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

Character Set Not Specified

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/Scripts/%2Cx.support.html5Clone%26%26e.innerHTML%26%26%21x.trim(t.innerHTML** |
| **Risk** | Info |

**Request**

[**GET /Scripts/%2Cx.support.html5Clone%26%26e.innerHTML%26%26%21x.trim(t.innerHTML**](about:blank)

**Resource Content**

|  |
| --- |
| /Scripts/%2Cx.support.html5Clone%26%26e.innerHTML%26%26%21x.trim(t.innerHTML |

**Discussion**

Vega has detected that the resource has not specified a character set in the response. If the character set is not specified, the browser may make assumptions about the character set based on resource content. This may present a security concern if the affected resource contains dynamically-generated content that originates from users. In such a case, malicious users may potentially take advantage of how specific browsers interpret characters to cause malicious content to be rendered. For example, an attacker may be able to bypass a cross-site scripting filter by encoding their malicious payload in an alternate character set, which may be executed depending on how the browser interprets the encoded content.

**Remediation**

* Specify a well-defined character set (such as UTF-8) within the response header content-type or the response body.

**References**

Some additional links with relevant information published by third-parties:

* [**OWASP Top Ten Cheat Sheet**](https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

Character Set Not Specified

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/Scripts/this%2Cr%2Ci.html(** |
| **Risk** | Info |

**Request**

[**GET /Scripts/this%2Cr%2Ci.html(**](about:blank)

**Resource Content**

|  |
| --- |
| /Scripts/this%2Cr%2Ci.html( |

**Discussion**

Vega has detected that the resource has not specified a character set in the response. If the character set is not specified, the browser may make assumptions about the character set based on resource content. This may present a security concern if the affected resource contains dynamically-generated content that originates from users. In such a case, malicious users may potentially take advantage of how specific browsers interpret characters to cause malicious content to be rendered. For example, an attacker may be able to bypass a cross-site scripting filter by encoding their malicious payload in an alternate character set, which may be executed depending on how the browser interprets the encoded content.

**Remediation**

* Specify a well-defined character set (such as UTF-8) within the response header content-type or the response body.

**References**

Some additional links with relevant information published by third-parties:

* [**OWASP Top Ten Cheat Sheet**](https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

Character Set Not Specified

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/Scripts/window.html5** |
| **Risk** | Info |

**Request**

[**GET /Scripts/window.html5**](about:blank)

**Resource Content**

|  |
| --- |
| /Scripts/window.html5 |

**Discussion**

Vega has detected that the resource has not specified a character set in the response. If the character set is not specified, the browser may make assumptions about the character set based on resource content. This may present a security concern if the affected resource contains dynamically-generated content that originates from users. In such a case, malicious users may potentially take advantage of how specific browsers interpret characters to cause malicious content to be rendered. For example, an attacker may be able to bypass a cross-site scripting filter by encoding their malicious payload in an alternate character set, which may be executed depending on how the browser interprets the encoded content.

**Remediation**

* Specify a well-defined character set (such as UTF-8) within the response header content-type or the response body.

**References**

Some additional links with relevant information published by third-parties:

* [**OWASP Top Ten Cheat Sheet**](https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

Character Set Not Specified

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/Scripts/window.HTMLDataListElement** |
| **Risk** | Info |

**Request**

[**GET /Scripts/window.HTMLDataListElement**](about:blank)

**Resource Content**

|  |
| --- |
| /Scripts/window.HTMLDataListElement |

**Discussion**

Vega has detected that the resource has not specified a character set in the response. If the character set is not specified, the browser may make assumptions about the character set based on resource content. This may present a security concern if the affected resource contains dynamically-generated content that originates from users. In such a case, malicious users may potentially take advantage of how specific browsers interpret characters to cause malicious content to be rendered. For example, an attacker may be able to bypass a cross-site scripting filter by encoding their malicious payload in an alternate character set, which may be executed depending on how the browser interprets the encoded content.

**Remediation**

* Specify a well-defined character set (such as UTF-8) within the response header content-type or the response body.

**References**

Some additional links with relevant information published by third-parties:

* [**OWASP Top Ten Cheat Sheet**](https://www.owasp.org/index.php/OWASP_Top_Ten_Cheat_Sheet)

[**Top**](about:blank#titlesection)

C:\Program Files (x86)\Vega\configuration\org.eclipse.osgi\bundles\20\2\.cp\icons\bannerLogo.pngOpen Source Web Security Platform

Cookie HttpOnly Flag Not Set

**At a glance**

|  |  |
| --- | --- |
| **Classification** | [**Information**](about:blank#description) |
| **Resource** | **/** |
| **Risk** | Info |

**Request**

[**GET /**](about:blank)

**Resource Content**

|  |
| --- |
| ARRAffinity=c7b6562ce70fbefbf2484bdff687cec172010b84562cd41b74802d67f079f8d0;Path=/;Domain=adminus.azurewebsites.net |

**Discussion**

Vega has detected that this cookie was set without the HttpOnly flag. When this flag is not present, it is possible to access the cookie via client-side script code. The HttpOnly flag is a security measure that can help mitigate the risk of cross-site scripting attacks that target session cookies of the victim. If the HttpOnly flag is set and the browser supports this feature, attacker-supplied script code will not be able to access the cookie.

**Remediation**

* When creating the cookie in the code, set the HttpOnly flag to true.

**References**

Some additional links with relevant information published by third-parties:

* [**HttpOnly OWASP Reference**](https://www.owasp.org/index.php/HttpOnly)

[**Top**](about:blank#titlesection)