**ESCANEO DE VULNERABILIDADES**

Escaneo realizado a la aplicación <https://adminus.azurewebsites.net/> desde un ambiente local mediante la herramienta [OWASP ZAP](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project), el cual actúa como Proxy Interceptor permitiendo ver todas las peticiones y respuestas sobre una aplicación web, realiza un escaneo activo sobre la aplicación permitiendo identificar diferentes tipos de vulnerabilidad.

**ZAP Scanning Report**

**Summary of Alerts**

|  |  |
| --- | --- |
| **Risk Level** | **Number of Alerts** |
| [High](file:///C:\Users\EXTIGL~1\AppData\Local\Temp\vulnerabilities-scan-zap%20(2).html#high) | 0 |
| [Medium](file:///C:\Users\EXTIGL~1\AppData\Local\Temp\vulnerabilities-scan-zap%20(2).html#medium) | 1 |
| [Low](file:///C:\Users\EXTIGL~1\AppData\Local\Temp\vulnerabilities-scan-zap%20(2).html#low) | 11 |
| [Informational](file:///C:\Users\EXTIGL~1\AppData\Local\Temp\vulnerabilities-scan-zap%20(2).html#info) | 9 |

**Alert Detail**

|  |  |
| --- | --- |
| **Medium (Warning)** | **Application Error disclosure** |
| Description | This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application.The alert could be a false positive if the error message is found inside a documentation page. |
|  | |
| URL | http://localhost:52842/Errors?aspxerrorpath=/ |
| Parameter | N/A |
| Attack | HTTP 500 Internal server error |
|  | |
| Solution | Review the source code of this page |
| Reference |  |
| CWE Id | 200 |
| WASC Id | 13 |

|  |  |
| --- | --- |
| **Low (Warning)** | **X-Content-Type-Options header missing** |
| Description | The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'.  This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type.  Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing. |
|  | |
| URL | http://localhost:52842/ |
|  | |
| Solution | Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing. |
| Reference |  |

|  |  |
| --- | --- |
| **Low (Warning)** | **X-Content-Type-Options header missing** |
| Description | The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'.  This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type.  Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing. |
|  | |
| URL | http://localhost:52842/Content/Site.css |
|  | |
| Solution | Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing. |
| Reference |  |

|  |  |
| --- | --- |
| **Low (Warning)** | **X-Content-Type-Options header missing** |
| Description | The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'.  This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type.  Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing. |
|  | |
| URL | http://localhost:52842/Content/font-awesome.min.css |
|  | |
| Solution | Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing. |
| Reference |  |

|  |  |
| --- | --- |
| **Low (Warning)** | **X-Content-Type-Options header missing** |
| Description | The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'.  This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type.  Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing. |
|  | |
| URL | http://localhost:52842/Content/bootstrap.min.css |
|  | |
| Solution | Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing. |
| Reference |  |

|  |  |
| --- | --- |
| **Low (Warning)** | **X-Content-Type-Options header missing** |
| Description | The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'.  This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type.  Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing. |
|  | |
| URL | http://localhost:52842/Scripts/modernizr-2.6.2.js |
|  | |
| Solution | Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing. |
| Reference |  |

|  |  |
| --- | --- |
| **Low (Warning)** | **X-Content-Type-Options header missing** |
| Description | The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'.  This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type.  Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing. |
|  | |
| URL | http://localhost:52842/Scripts/jquery-1.10.2.min.js |
|  | |
| Solution | Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing. |
| Reference |  |

|  |  |
| --- | --- |
| **Low (Warning)** | **X-Content-Type-Options header missing** |
| Description | The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'.  This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type.  Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing. |
|  | |
| URL | http://localhost:52842/Scripts/jquery.validate.min.js |
|  | |
| Solution | Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing. |
| Reference |  |

|  |  |
| --- | --- |
| **Low (Warning)** | **X-Content-Type-Options header missing** |
| Description | The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'.  This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type.  Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing. |
|  | |
| URL | http://localhost:52842/Scripts/jquery.validate.unobtrusive.min.js |
|  | |
| Solution | Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing. |
| Reference |  |

|  |  |
| --- | --- |
| **Low (Warning)** | **X-Content-Type-Options header missing** |
| Description | The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'.  This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type.  Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing. |
|  | |
| URL | http://localhost:52842/Scripts/bootstrap.min.js |
|  | |
| Solution | Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing. |
| Reference |  |

|  |  |
| --- | --- |
| **Low (Warning)** | **Content-Type header missing** |
| Description | Content-Type header missing |
|  | |
| URL | http://localhost:52842/ |
|  | |
| Solution | Ensure each page is setting the specific and appropriate content-type value for the content being delivered |
| Reference | http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx |

|  |  |
| --- | --- |
| **Low (Warning)** | **X-Content-Type-Options header missing** |
| Description | The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'.  This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type.  Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing. |
|  | |
| URL | http://localhost:52842/Errors?aspxerrorpath=/ |
|  | |
| Solution | Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.  If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing. |
| Reference |  |

|  |  |
| --- | --- |
| **Informational (Warning)** | **X-Frame-Options header not set** |
| Description | X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks |
|  | |
| URL | http://localhost:52842/Content/Site.css |
|  | |
| Solution | Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers). |
| Reference | http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx?Redirected=true |

|  |  |
| --- | --- |
| **Informational (Warning)** | **X-Frame-Options header not set** |
| Description | X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks |
|  | |
| URL | http://localhost:52842/Content/font-awesome.min.css |
|  | |
| Solution | Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers). |
| Reference | http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx?Redirected=true |

|  |  |
| --- | --- |
| **Informational (Warning)** | **X-Frame-Options header not set** |
| Description | X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks |
|  | |
| URL | http://localhost:52842/Content/bootstrap.min.css |
|  | |
| Solution | Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers). |
| Reference | http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx?Redirected=true |

|  |  |
| --- | --- |
| **Informational (Warning)** | **X-Frame-Options header not set** |
| Description | X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks |
|  | |
| URL | http://localhost:52842/Scripts/modernizr-2.6.2.js |
|  | |
| Solution | Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers). |
| Reference | http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx?Redirected=true |

|  |  |
| --- | --- |
| **Informational (Warning)** | **X-Frame-Options header not set** |
| Description | X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks |
|  | |
| URL | http://localhost:52842/Scripts/jquery-1.10.2.min.js |
|  | |
| Solution | Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers). |
| Reference | http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx?Redirected=true |

|  |  |
| --- | --- |
| **Informational (Warning)** | **X-Frame-Options header not set** |
| Description | X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks |
|  | |
| URL | http://localhost:52842/Scripts/jquery.validate.min.js |
|  | |
| Solution | Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers). |
| Reference | http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx?Redirected=true |

|  |  |
| --- | --- |
| **Informational (Warning)** | **X-Frame-Options header not set** |
| Description | X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks |
|  | |
| URL | http://localhost:52842/Scripts/jquery.validate.unobtrusive.min.js |
|  | |
| Solution | Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers). |
| Reference | http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx?Redirected=true |

|  |  |
| --- | --- |
| **Informational (Warning)** | **X-Frame-Options header not set** |
| Description | X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks |
|  | |
| URL | http://localhost:52842/Scripts/bootstrap.min.js |
|  | |
| Solution | Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers). |
| Reference | http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx?Redirected=true |

|  |  |
| --- | --- |
| **Informational (Warning)** | **X-Frame-Options header not set** |
| Description | X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks |
|  | |
| URL | http://localhost:52842/Errors?aspxerrorpath=/ |
|  | |
| Solution | Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers). |
| Reference | http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx?Redirected=true |