# ZAP Scanning Report

## Summary of Alerts

| Risk Level | Number of Alerts |
|---|---|
| High | 0 |
| Medium | 1 |
| Low | 5 |
| Informational | 0 |

## Alert Detail

| Medium (Medium) | 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://dev.investorstatelawguide.com/Home/UserNotSubmittingNotePadDetails |
| Method | GET |
| Evidence | HTTP/1.1 500 Internal Server Error |
| URL | http://dev.investorstatelawguide.com/ResearchTools/inputAll |
| Method | POST |
| Evidence | HTTP/1.1 500 Internal Server Error |
| URL | http://dev.investorstatelawguide.com/Home/Register?Length=0 |
| Method | GET |
| Evidence | HTTP/1.1 500 Internal Server Error |
| URL | http://dev.investorstatelawguide.com/Home/AddNewNotePadUser?Continue=Y |
| Method | POST |
| Evidence | HTTP/1.1 500 Internal Server Error |
| URL | http://dev.investorstatelawguide.com/Home/AddNewNotePadUser?Continue=Y |
| Method | GET |
| Evidence | HTTP/1.1 500 Internal Server Error |
| Instances | 5 |
| Solution | Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user. |
| Reference | |
| CWE Id | 200 |
| WASC Id | 13 |
| Source ID | 3 |

| | |
|---|---|
| Source ID | 3 |

| Low (Medium) | 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://detectportal.firefox.com/success.txt |
| Method | GET |
| Parameter | X-Content-Type-Options |
| Instances | 1 |
| 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.<br><br>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. |
| Other information | This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.<br><br>At "High" threshold this scanner will not alert on client or server error responses. |
| Reference | http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx<br><br>https://www.owasp.org/index.php/List_of_useful_HTTP_headers |
| CWE Id | 16 |
| WASC Id | 15 |
| Source ID | 3 |

| Low (Medium) | Web Browser XSS Protection Not Enabled |
|---|---|
| Description | Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server |
| URL | http://dev.investorstatelawguide.com/ResearchTools |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/sitemap.xml |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=r&searchType&toc=termsPhrases |

| | |
|---|---|
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=n&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/Scripts/lz-string.js |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/blank.html |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=a&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=p&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/Scripts/ |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/FancyBoxNew/ |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=l&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/Home/UserSession |
| Method | GET |

| | |
|---|---|
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/ |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/nonMember/nonMember?Id=81 |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/Home/EditNewNotePadUser?Continue=Y |
| Method | POST |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/subscribers/LogTheLogoutSessionTime |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=e&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/ResearchTools/fts_help |
| Method | GET |
| Parameter | X-XSS-Protection |
| URL | http://dev.investorstatelawguide.com/Home/Login?id=201&returnUrl=/ResearchTools/ArticleCitator?cat=investmenttreaty&subcat=nafta&toc=content |
| Method | GET |
| Parameter | X-XSS-Protection |
| Instances | 112 |
| Solution | Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'. |
| Other information | The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it:<br><br>X-XSS-Protection: 1; mode=block<br><br>X-XSS-Protection: 1; report=http://www.example.com/xss<br><br>The following values would disable it:<br><br>X-XSS-Protection: 0 |

| | |
|---|---|
| | The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).<br><br>Note that this alert is only raised if the response body could potentially contain an XSS payload (with a text-based content type, with a non-zero length). |
| Reference | https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet<br><br>https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/ |
| CWE Id | 933 |
| WASC Id | 14 |
| Source ID | 3 |

| **Low (Medium)** | **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://dev.investorstatelawguide.com/Scripts/excanvas.js |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/JurisprudenceCitators?id=11&type=gatt |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/subscribers/LogPageCountForUserSession |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/FullTextSearch?toc=content&id=97&tab=r |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/User/CheckAgreementNavigatorActive |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/themes/base/jquery.ui.resizable.css |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/User/CheckAgreementNavigatorActive |

| | |
|---|---|
| Method | POST |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/themes/base/jquery.ui.button.css |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/themes/base/jquery.ui.theme.css |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=k&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/Home/Login?id=201&returnUrl=/ResearchTools/ArticleCitator?cat=investmenttreaty&subcat=fta&toc=content |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=a&searchType=T&toc=termsPhrases |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/Home/Login?id=201&returnUrl=/ResearchTools/ArticleCitator?cat=investmenttreaty&subcat=intlawrules&toc=content |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/Home/Login?Logout=Yes&autologin=n |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=m&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/Scripts/MicrosoftMvcValidation.js |
| Method | GET |

| | |
|---|---|
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/NonMembers/UserTabs?id=86 |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/Home/Login?Logout=Yes&autologin=n |
| Method | POST |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/Scripts/dhtmlwindow_1_2.js |
| Method | GET |
| Parameter | X-Content-Type-Options |
| URL | http://dev.investorstatelawguide.com/Design/CSS/style.css |
| Method | GET |
| Parameter | X-Content-Type-Options |
| Instances | 164 |
| 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.<br><br>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. |
| Other information | This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.<br><br>At "High" threshold this scanner will not alert on client or server error responses. |
| Reference | http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx<br><br>https://www.owasp.org/index.php/List_of_useful_HTTP_headers |
| CWE Id | 16 |
| WASC Id | 15 |
| Source ID | 3 |

| **Low (Medium)** | **Password Autocomplete in Browser** |
|---|---|
| Description | The AUTOCOMPLETE attribute is not disabled on an HTML FORM/INPUT element containing password type input. Passwords may be stored in browsers and retrieved. |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=c&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |

| | |
|---|---|
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/User/Welcome |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=a&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=z&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=r&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?id=201&returnUrl=/ResearchTools/ArticleCitator?cat=investmenttreaty&subcat=intlawrules&toc=content |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?id=201&returnUrl=/ResearchTools/ArticleCitator?cat=investmenttreaty&subcat=fta&toc=content |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=v&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |

| | |
|---|---|
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/JurisprudenceCitators?id=11&type=all |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?id=201&returnUrl=/ResearchTools/ArticleCitator?cat=investmenttreaty&subcat=nafta&toc=content |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?Logout=Yes&autologin=n |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=e&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?id=201&returnUrl=/ResearchTools/ArticleCitator?cat=investmenttreaty&subcat=other&toc=content |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=a&searchType=T&toc=termsPhrases |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?Logout=Yes&autologin=n |
| Method | POST |
| Parameter | Password |

| | |
|---|---|
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=i&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/JurisprudenceCitators?id=11&type=gatt |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=k&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=p&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/TermsPhrases?letter=q&searchType&toc=termsPhrases |
| Method | GET |
| Parameter | Password |
| Evidence | <input class="textbox" id="Password" name="Password" type="password" value="" /> |
| Instances | 47 |
| Solution | Turn off the AUTOCOMPLETE attribute in forms or individual input elements containing password inputs by using AUTOCOMPLETE='OFF'. |
| Reference | http://www.w3schools.com/tags/att_input_autocomplete.asp<br><br>https://msdn.microsoft.com/en-us/library/ms533486%28v=vs.85%29.aspx |
| CWE Id | 525 |
| WASC Id | 15 |
| Source ID | 3 |

| **Low (Medium)** | **Cookie No HttpOnly Flag** |
|---|---|
| Description | A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and |

| | |
|---|---|
| | can be transmitted to another site. If this is a session cookie then session hijacking may be possible. |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/FullTextSearch?toc=content&id=97&tab=r |
| Method | POST |
| Parameter | RePassword |
| Evidence | Set-Cookie: RePassword |
| URL | http://dev.investorstatelawguide.com/Home/Login?Logout=Yes&autologin=n |
| Method | GET |
| Parameter | Password |
| Evidence | Set-Cookie: Password |
| URL | http://dev.investorstatelawguide.com/Home/Login?Logout=Yes&autologin=n |
| Method | GET |
| Parameter | UserId |
| Evidence | Set-Cookie: UserId |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/FullTextSearch?toc=content&id=97&tab=r |
| Method | POST |
| Parameter | ReUserId |
| Evidence | Set-Cookie: ReUserId |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/FullTextSearch?toc=content&id=97&tab=r |
| Method | POST |
| Parameter | Password |
| Evidence | Set-Cookie: Password |
| URL | http://dev.investorstatelawguide.com/Home/Login?returnUrl=/ResearchTools/FullTextSearch?toc=content&id=97&tab=r |
| Method | POST |
| Parameter | UserId |
| Evidence | Set-Cookie: UserId |
| Instances | 6 |
| Solution | Ensure that the HttpOnly flag is set for all cookies. |
| Reference | http://www.owasp.org/index.php/HttpOnly |
| CWE Id | 16 |
| WASC Id | 13 |
| Source ID | 3 |

| | |
|---|---|
| Source ID | 3 |