ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	2
Medium	3
Low	10
Informational	0

Alert Detail

High (Medium)	Remote OS Command Injection
Description	Attack technique used for unauthorized execution of operating system commands. This attack is possible when an application accepts untrusted input to build operating system commands in an insecure manner involving improper data sanitization, and/or improper calling of external programs.
URL	http://dev.investorstatelawguide.com/assets/images/Team/liam-murphy-burke.png?query=query%27%3Bstart-sleep+-s+15
Method	GET
Parameter	query
Attack	query';start-sleep -s 15
Instances	1
Solution	If at all possible, use library calls rather than external processes to recreate the desired functionality. Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict which files can be accessed in a particular directory or which commands can be executed by your software. OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission in the Java SecurityManager allows you to specify restrictions on file operations. This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise. For any data that will be used to generate a command to be executed, keep as much of that data out of external control as possible. For example, in web applications, this may require storing the command locally in the session's state instead of sending it out to the client in a hidden form field. Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, consider using the ESAPI Encoding control or a similar tool, library, or framework. These will help the programmer encode outputs in a manner less prone to error. If you need to use dynamically-generated query strings or commands in spite of the risk, properly quote arguments and escape any special characters within those arguments. The most conservative approach is to escape or filter all characters that do not pass an extremely strict whitelist (such as everything that is not alphanumeric or white space). If some special characters are still needed, such as white space, wrap each argument in quotes after the escaping/filtering step. Be careful of argument injection. If the program to be executed allows arguments to be specified within an input file or from standard input, then consider using that mode to pass arguments instead of the command line. If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated. Some languages offer multiple functions that can be used to invoke commands. Where possible, identify any function that invokes a command shell using a single string, and replace it with a function that requires individual arguments. These functions typically perform appropriate quoting and filtering of arguments. For example, in C, the system() function accepts a string that contains the entire command to be executed, whereas execl(), execve(), and others require an array of strings, one for each argument. In Windows, CreateProcess() only accepts one command at a time. In Perl, if system() is provided with an array of arguments, then it will quote each of the arguments. Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. Reject any input that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do not rely on a blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inputs, syntax, consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains alphanumeric characters, but it is not valid if you are expecting colors such as "red" or "blue." When constructing OS command strings, use stringent whitelists that limit the character set based on the expected value of the parameter in the request. This will indirectly limit the scope of an attack, but this technique is less important than proper output encoding and escaping. Note that proper output encoding, escaping, and quoting is the most effective solution for preventing OS command injection, although input validation may provide some defense-in-depth. This is because it effectively limits what will appear in output. Input validation will not always prevent OS command injection, especially if you are required to support free-form text fields that could contain arbitrary characters. For example, when invoking a mail program, you might need to allow the subject field to contain otherwise-dangerous inputs like ";" and ">" characters, which would need to be escaped or otherwise handled. In this case, stripping the character might reduce the risk of OS command injection, but it would produce incorrect behavior because the subject field would not be recorded as the user intended. This might seem to be a minor inconvenience, but it could be more important when the program relies on well-structured subject lines in order to pass messages to other components. Even if you make a mistake in your validation (such as forgetting one out of 100 input fields), appropriate encoding is still likely to protect you from injection-based attacks. As long as it is not done in isolation, input validation is still a useful technique, since it may significantly reduce your attack surface, allow you to detect some attacks, and provide other security benefits that proper encoding does not address.
Reference	http://cwe.mitre.org/data/definitions/78.html https://www.owasp.org/index.php/Command_Injection
CWE Id	78
WASC Id	31

Source ID	1

High (Medium)	Path Traversal
Description	The Path Traversal attack technique allows an attacker access to files, directories, and commands that potentially reside outside the web document root directory. Ar manipulate a URL in such a way that the web site will execute or reveal the contents of arbitrary files anywhere on the web server. Any device that exposes an HTTP- is potentially vulnerable to Path Traversal. Most web sites restrict user access to a specific portion of the file-system, typically called the "web document root" or "CGI root" directory. These directories contain intended for user access and the executable necessary to drive web application functionality. To access files or execute commands anywhere on the file-system, Pat attacks will utilize the ability of special-characters sequences. The most basic Path Traversal attack uses the "../" special-character sequence to alter the resource location requested in the URL. Although most popular web serve this technique from escaping the web document root, alternate encodings of the "../" sequence may help bypass the security filters. These method variations include Unicode-encoding ("..%u2216" or "..%c0%af") of the forward slash character, backslash characters ("..\") on Windows-based servers, URL encoded characters "%2 double URL encoding ("..%255c") of the backslash character. Even if the web server properly restricts Path Traversal attempts in the URL path, a web application itself may still be vulnerable due to improper handling of user-sup is a common problem of web applications that use template mechanisms or load static text from files. In variations of the attack, the original URL parameter value is the file name of one of the web application's dynamic scripts. Consequently, the results can reveal source code because the file is interpreted as text instead of an ex These techniques often employ additional special characters such as the dot (".") to reveal the listing of the current working directory, or "%00" NULL characters in o rudimentary file extension checks.
URL	http://dev.investorstatelawguide.com/start-your-trial?City=ZAP&Country=Albania&Email=start-your-trial&EnableEditProfile=1&Firm_Institution=ZAP&FirstName=ZAP&I_am_18years_or_Older=1&LastName=ZAP&Position=ZAP&SheduleTutorial=false&TermsConditions recaptcha-response=&id=54&save=y&signup=y&toc=content
Method	POST
Parameter	Email
Attack	start-your-trial
Instances	1
Solution	Assume all input is malicious. Use an "accept known good" input validation strategy, i.e., use a whitelist of acceptable inputs that strictly conform to specifications. R that does not strictly conform to specifications, or transform it into something that does. Do not rely exclusively on looking for malicious or malformed inputs (i.e., do blacklist). However, blacklists can be useful for detecting potential attacks or determining which inputs are so malformed that they should be rejected outright. When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra input consistency across related fields, and conformance to business rules. As an example of business rule logic, "boat" may be syntactically valid because it only contains characters, but it is not valid if you are expecting colors such as "red" or "blue." For filenames, use stringent whitelists that limit the character set to be used. If feasible, only allow a single "." character in the filename to avoid weaknesses, and exc separators such as "/". Use a whitelist of allowable file extensions. Warning: if you attempt to cleanse your data, then do so that the end result is not in the form that can be dangerous. A sanitizing mechanism can remove characters ';' which may be required for some exploits. An attacker can try to fool the sanitizing mechanism into "cleaning" data into a dangerous form. Suppose the attacker inj a filename (e.g. "sensi.tiveFile") and the sanitizing mechanism removes the character resulting in the valid filename, "sensitiveFile". If the input data are now assumed the file may be compromised. Inputs should be decoded and canonicalized to the application's current internal representation before being validated. Make sure that your application does not dec input twice. Such errors could be used to bypass whitelist schemes by introducing dangerous inputs after they have been checked. Use a built-in path canonicalization function (such as realpath() in C) that produces the canonical version of the pathname, which effectively removes ".." sequences a links. Run your code using the lowest privileges that are required to accomplish the necessary tasks. If possible, create isolated accounts with limited privileges that are on single task. That way, a successful attack will not immediately give the attacker access to the rest of the software or its environment. For example, database applicati to run as the database administrator, especially in day-to-day operations. When the set of acceptable objects, such as filenames or URLs, is limited or known, create a mapping from a set of fixed input values (such as numeric IDs) to the ac URLs, and reject all other inputs. Run your code in a "jail" or similar sandbox environment that enforces strict boundaries between the process and the operating system. This may effectively restrict be accessed in a particular directory or which commands can be executed by your software. OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission SecurityManager allows you to specify restrictions on file operations. This may not be a feasible solution, and it only limits the impact to the operating system; the rest of your application may still be subject to compromise.
Reference	http://projects.webappsec.org/Path-Traversal http://cwe.mitre.org/data/definitions/22.html
CWE Id	22
WASC Id	33
Source ID	1

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	https://dev.investorstatelawguide.com/start-your-trial
Method	POST
Evidence	HTTP/1.1 500 Internal Server Error
Instances	1
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

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/Register?Length=0
Method	POST
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/start-your-trial
Method	POST
Evidence	HTTP/1.1 500 Internal Server Error
Instances	2
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

Medium (Medium)	Format String Error
Description	A Format String error occurs when the submitted data of an input string is evaluated as a command by the application.
URL	http://dev.investorstatelawguide.com/start-your-trial? City=ZAP&Country=Albania&Email=ZAP+%251%21s%252%21s%253%21s%254%21s%255%21s%256%21s%257%21s%258%21s%259%21s%2510%21s%2 response=&id=54&save=y&signup=y&toc=content
Method	POST
Parameter	Email
Attack	ZAP %1!s%2!s%3!s%4!s%5!s%6!s%7!s%8!s%9!s%10!s%11!s%12!s%13!s%14!s%15!s%16!s%17!s%18!s%19!s%20!s%21!n%22!n%23!n%24!n%25!n%26!n%2
URL	http://dev.investorstatelawguide.com/Home/Register? City=ZAP&Country=Albania&Email=ZAP+%251%21s%252%21s%253%21s%254%21s%255%21s%256%21s%257%21s%258%21s%259%21s%2510%21s%2 recaptcha-response=&id=54&save=y&signup=y&toc=content
Method	POST
Parameter	Email
Attack	ZAP %1!s%2!s%3!s%4!s%5!s%6!s%7!s%8!s%9!s%10!s%11!s%12!s%13!s%14!s%15!s%16!s%17!s%18!s%19!s%20!s%21!n%22!n%23!n%24!n%25!n%26!n%2
Instances	2
Solution	Rewrite the background program using proper deletion of bad character strings. This will require a recompile of the background executable.
Other information	Potential Format String Error. The script closed the connection on a microsoft format string error
Reference	https://www.owasp.org/index.php/Format_string_attack
CWE Id	134
WASC Id	6
Source ID	1

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	https://dev.investorstatelawguide.com/about-islg/Liam_Murphy_Burke
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/notepad-login
Method	POST
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/about-islg/Hassan_Kamalinejad
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/assets/images/Team/ProfilePlaceholder.png
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/about-islg/Andres_Felipe
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/assets/images/product/fts.png
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/about-islg/Christopher_Thomas

Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/about-islg/Csaba_Kovacs
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/assets/images/Team/laura-yvonne-zielinski.png
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/resources-events
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/about-islg/Alejandro_Barragan
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/assets/images/Home/marci-hoffman.png
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/about-islg/Paul_Moon
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/contact-us
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/Home/ForGetUserName?token=%2fJJ1P12gJvRpftktHjszEg%3d%3d
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/notepad-login
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/assets/images/Team/csaba-kovacs.png
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/assets/images/Home/clients/Curtis.png
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/assets/images/Team/marysia-raptis.png
Method	GET
Parameter	X-Content-Type-Options
URL	https://dev.investorstatelawguide.com/admin/adminlogin
Method	GET
Parameter	X-Content-Type-Options
Instances	140
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.
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. 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 https://www.owasp.org/index.php/List_of_useful_HTTP_headers
CWE Id	16
WASC Id	15
Source ID	3

Low (Medium)	**Incomplete or No Cache-control and Pragma HTTP Header Set**
Description	The cache-control and pragma HTTP header have not been set properly or are missing allowing the browser and proxies to cache content.
URL	https://dev.investorstatelawguide.com/about-islg/Olga_Boltenko
Method	GET
Parameter	Cache-Control

Evidence	private
URL	https://dev.investorstatelawguide.com/
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/admin/adminlogin
Method	POST
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/about-islg/Christopher_Thomas
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/admin/adminlogin
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/about-islg/Alejandro_Barragan
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/about-islg/Andrew_Newcombe
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/about-islg/Liam_Murphy_Burke
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/Home/ForGetPassWord?Length=0
Method	POST
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/about-islg/Andres_Felipe
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/Home/ForGetPassWord?Length=0
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/Home/ForGetUserName?token=%2fJJ1P12gJvRpftktHjszEg%3d%3d
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/contact-us
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/about-islg/Harpreet_K_Dhillon
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/about-islg/Paul_Moon
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/about-islg/Irit_Weinfeld
Method	GET

Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/resources-events
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/start-your-trial
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/about-islg/Csaba_Kovacs
Method	GET
Parameter	Cache-Control
Evidence	private
URL	https://dev.investorstatelawguide.com/notepad-login
Method	POST
Parameter	Cache-Control
Evidence	private
Instances	63
Solution	Whenever possible ensure the cache-control HTTP header is set with no-cache, no-store, must-revalidate; and that the pragma HTTP header is set with no-cache.
Reference	https://www.owasp.org/index.php/Session_Management_Cheat_Sheet#Web_Content_Caching
CWE Id	525
WASC Id	13
Source ID	3

Low (Medium)	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://dev.investorstatelawguide.com/about-islg/Ximena_Iturriaga
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/about-islg/Madalena_Beaudet
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/Views/MasterPages/image/Gear-Favicon.ico
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/recaptcha/api/fallback?k=6Le-wvkSAAAAAPBMRTvw0Q4Muexq9bi0DJwx_mJ-
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/start-your-trial?City=ZAP&Country=Albania&Email=ZAP&EnableEditProfile=1&Firm_Institution=ZAP&FirstName=ZAP&I_am_18years_or_Older=1&LastName=ZAP&Position=ZAP&Sh recaptcha-response&id=54&save=y&signup=y&toc=content
Method	POST
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/about-islg
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/about-islg/Jeremy_Bocock
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/Home/ForGetUserName?Length=0
Method	POST
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js

Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/start-your-trial?City=ZAP&Country=Albania&Email=ZAP&EnableEditProfile=1&Firm_Institution=ZAP&FirstName=ZAP&I_am_18years_or_Older=1&LastName=ZAP&Position=ZAP&Sh recaptcha-response&id=54&save=y&signup=y&toc=content
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/assets/icons/mstile-150x150.png
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/contact-us
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=reCAPTCHA_site_key
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=reCAPTCHA_site_key"></script>
URL	https://dev.investorstatelawguide.com/Home/ForGetUserName?Length=0
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/about-islg/Laura_Yvonne_Zielinski
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/Views/Scripts/jquery-ui.js
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/resources-events
Method	GET
Parameter	https://platform.twitter.com/widgets.js
Evidence	<script async="" src="https://platform.twitter.com/widgets.js" charset="utf-8"></script>
URL	https://dev.investorstatelawguide.com/about-islg/Eleo_Szulc
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/about-islg/Ivaylo_Dimitrov
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/about-islg/Sapna_Jhangiani
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/about-islg/Jennifer_Radford
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	https://dev.investorstatelawguide.com/product
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
Instances	63
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
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	https://dev.investorstatelawguide.com/about-islg/Sapna_Jhangiani
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/about-islg/Jennifer_Radford
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/contact-us?g-recaptcha-response
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/about-islg/Peter_Nikitin
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/assets/icons/android-chrome-192x192.png
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/ResearchTools/ShowDescription?Id=294
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/assets/icons/apple-touch-icon.png
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/about-islg/Greg_Tereposky
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/ResearchTools/ShowDescription?Id=249
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/contactus
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/about-islg/Cameron_Mowatt
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/about-islg/Nafiseh_Arghandeh
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/product
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/admin/adminlogin
Method	POST
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/about-islg/Andrew_Newcombe
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/admin/adminlogin
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/about-islg/Ximena_Iturriaga
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/about-islg/Christopher_Thomas
Method	GET
Parameter	X-XSS-Protection
URL	https://dev.investorstatelawguide.com/about-islg
Method	GET

Parameter	X-XSS-Protection
Instances	62
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: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). 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 https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3

Low (Medium)	**Cookie Without Secure Flag**
Description	A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.
URL	https://dev.investorstatelawguide.com/notepad-login
Method	GET
Parameter	UserId
Evidence	Set-Cookie: UserId
URL	https://dev.investorstatelawguide.com/notepad-login
Method	GET
Parameter	Password
Evidence	Set-Cookie: Password
Instances	2
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Reference	http://www.owasp.org/index.php/Testing_for_cookies_attributes_(OWASP-SM-002)
CWE Id	614
WASC Id	13
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	https://dev.investorstatelawguide.com/notepad-login
Method	GET
Parameter	UserId
Evidence	Set-Cookie: UserId
URL	https://dev.investorstatelawguide.com/notepad-login
Method	GET
Parameter	Password
Evidence	Set-Cookie: Password
Instances	2
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

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/about-islg/Eleo_Szulc
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/assets/images/product/Article-citator.png

Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/assets/scripts/min/sassquatch.min.js
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/CSS/font-awesome-4.7.0/css/font-awesome.min.css
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/assets/images/Home/map-relationships-icon.png
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/assets/images/Team/AndresTovar.png
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/assets/images/ISLG-logo.svg
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/assets/images/product/subjectnavgraphic.png
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/about-islg/Morgan_Maguire
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/assets/images/Team/ProfilePlaceholder.png
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/about-islg/Marysia_Raptis
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/assets/scripts/libraries/slick.js
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/about-islg/Jeremy_Bocock
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/assets/images/Team/laura-yvonne-zielinski.png
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/assets/styles/sassquatch.css
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/about-islg/Csaba_Kovacs
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/Home/Acknowledge
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/assets/images/Team/liam-murphy-burke.png
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/assets/images/Team/jennifer-radford.png
Method	GET
Parameter	X-Content-Type-Options
Instances	144
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.
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. 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 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/sitemap.xml
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/about-islg/Alejandro_Barragan
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/ResearchTools/ShowDescription?Id=249
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/Home/ForGetUserName?token=%2fJJ1P12gJvRpftktHjszEg%3d%3d
Method	POST
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/about-islg
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/ResearchTools/ShowDescription?Id=294
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/about-islg/Harpreet_K_Dhillon
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/about-islg/Olga_Boltenko
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/about-islg/Christopher_Thomas
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/about-islg/Irit_Weinfeld
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/about-islg/Andres_Felipe
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/Home/ForGetPassword?token=%2fJJ1P12gJvRpftktHjszEg%3d%3d
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/Home/ForGetUserName?token=%2fJJ1P12gJvRpftktHjszEg%3d%3d
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/Home/Register?Length=0
Method	POST
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/
Method	GET

Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/Home/ForGetUserName?Length=0
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/Home/ForGetPassword?token=%2fJJ1P12gJvRpftktHjszEg%3d%3d
Method	POST
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/about-islg/Marysia_Raptis
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/Home/ForGetUserName?Length=0
Method	POST
Parameter	X-XSS-Protection
Instances	69
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: X-XSS-Protection: 1; mode=block X-XSS-Protection: 1; report=http://www.example.com/xss The following values would disable it: X-XSS-Protection: 0 The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit). 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 https://blog.veracode.com/2014/03/guidelines-for-setting-security-headers/
CWE Id	933
WASC Id	14
Source ID	3

Low (Medium)	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	http://dev.investorstatelawguide.com/about-islg/Mark_Skilling
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/about-islg/Juliana_Sirotsky_Soria
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/Home/Register?City=ZAP&Country=Albania&Email=ZAP&EnableEditProfile=1&Firm_Institution=ZAP&FirstName=ZAP&I_am_18years_or_Older=1&LastName=ZAP&Length=0&Positio recaptcha-response&id=54&save=y&signup=y&toc=content
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/Home/ForGetPassWord?Length=0
Method	POST
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/resources-events
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/about-islg/Cameron_Mowatt
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/contactus
Method	GET

Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/about-islg/Nafiseh_Arghandeh
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/contact-us?g-recaptcha-response
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/Home/ForGetPassWord?Length=0
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/about-islg/Jennifer_Radford
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/about-islg/Sapna_Jhangiani
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/recaptcha/api/fallback?k=6Le-wvkSAAAAAPBMRTvw0Q4Muexq9bi0DJwx_mJ-
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/product
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/robots.txt
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/about-islg/Laura_Yvonne_Zielinski
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/about-islg/Diana_Ruiz
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
URL	http://dev.investorstatelawguide.com/contact-us?g-recaptcha-response
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?render=reCAPTCHA_site_key
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?render=reCAPTCHA_site_key"></script>
URL	http://dev.investorstatelawguide.com/resources-events
Method	GET
Parameter	https://platform.twitter.com/widgets.js
Evidence	<script async="" src="https://platform.twitter.com/widgets.js" charset="utf-8"></script>
URL	http://dev.investorstatelawguide.com/about-islg/Alejandro_Barragan
Method	GET
Parameter	https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js
Evidence	<script src="https://cdnjs.cloudflare.com/ajax/libs/jquery/3.3.1/jquery.min.js"></script>
Instances	71
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
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/notepad-login
Method	GET
Parameter	Password
Evidence	Set-Cookie: Password
URL	http://dev.investorstatelawguide.com/notepad-login
Method	GET
Parameter	UserId
Evidence	Set-Cookie: UserId
Instances	2
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