ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	4
Medium	2
Low	8
Informational	0

Alert Detail

High (Medium)	SQL Injection
Description	SQL injection may be possible.
URL	http://dev.investorstatelawguide.com/ResearchTools/SubjectNavigator?id=50&tab=r&toc=content+AND+1%3D1+--+
Method	GET
Parameter	toc
Attack	content AND 1=1 --
URL	http://dev.investorstatelawguide.com/User/disputedirectory/DisputeDocument?DocLanguage_English=1&DocumentLanguage=E&ID=10&aprule=&aprule_arbrule_lcia
Method	GET
Parameter	treaty_id
Attack	2-2
URL	http://dev.investorstatelawguide.com/User/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLangua 2&dispState=&disp_treaty=&doccat_1=1&doccat_12=1&doccat_13=1&doccat_15=1&doccat_16=1&doccat_17=1&doccat_18=1&doccat_2=1&doccat_21=1&doccat_
Method	GET
Parameter	defendingCountrydisp
Attack	2-2
URL	http://dev.investorstatelawguide.com/User/disputedirectory/DisputeDocument?DocLanguage_Spanish=1&DocumentLanguage=S&ID=10&aprule=&aprule_arbrule_lc
Method	GET
Parameter	treaty_id
Attack	2-2
URL	http://dev.investorstatelawguide.com/User/disputedirectory/DisputeDocument?DocLanguage_Spanish=1&DocumentLanguage=S&ID=10&aprule=&aprule_arbrule_lc
Method	GET
Parameter	defendingCountrydisp
Attack	2-2
URL	http://dev.investorstatelawguide.com/User/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLangua 2&dispState=&disp_treaty=&doccat_1=1&doccat_12=1&doccat_13=1&doccat_15=1&doccat_16=1&doccat_17=1&doccat_18=1&doccat_2=1&doccat_21=1&doccat_
Method	GET
Parameter	defendingCountrydisp
Attack	2-2
URL	http://dev.investorstatelawguide.com/User/disputedirectory/DisputeDocument? DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_German=1&DocLanguage_Spanish=1&DocLanguage_other=1&DocumentLa 2&treatycat=
Method	GET
Parameter	treaty_id
Attack	2-2
URL	http://dev.investorstatelawguide.com/User/disputedirectory/DisputeDocument? DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_German=1&DocLanguage_Spanish=1&DocLanguage_other=1&DocumentLa
Method	GET
Parameter	treaty_id
Attack	2-2
URL	http://dev.investorstatelawguide.com/User/disputedirectory/DisputeDocument?DocLanguage_English=1&DocumentLanguage=E&ID=10&aprule=&aprule_arbrule_lcia
Method	GET
Parameter	defendingCountrydisp
Attack	2-2
Instances	9
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries.

	If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply a 'whitelist' of allowed characters, or a 'blacklist' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Other information	The page results were successfully manipulated using the boolean conditions [content AND 1=1 --] and [content AND 1=2 --] The parameter value being modified was stripped from the HTML output for the purposes of the comparison Data was returned for the original parameter. The vulnerability was detected by successfully restricting the data originally returned, by manipulating the parameter
Reference	https://www.owasp.org/index.php/Top_10_2010-A1 https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
CWE Id	89
WASC Id	19
Source ID	1

High (Medium)	**SQL Injection - Microsoft SQL Server**
Description	SQL injection may be possible.
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDoc_AllDocList?ID=10&doclist=IC%2f0164%2f18%3bIC%2f0164%2f19&goback=%2fdisputedirector
Method	GET
Parameter	doclist
Attack	IC/0164/18;IC/0164/19') UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20Trust%20(Barbados)%20Ltd.%20v.%20Bolivarian%20Republic%20of%20Venez
Method	GET
Parameter	disputeId
Attack	885860) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20Tobago%20(ICSID%20Case%20No.%20ARB/01/14)&ID=10&Location=Trinidad%
Method	GET
Parameter	disputeId
Attack	663368) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20ARB/10/18)&%20Production%20Company%20Limited%20(%22Bapex%22)%2
Method	GET
Parameter	disputeId
Attack	1374689) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%2520Engineers%2520v.%2520Republic%2520of%2520Albania%2520(ICSID%252
Method	GET
Parameter	disputeId
Attack	705056) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20ARB/04/8)&ID=10&Location=Argentina%20-%20Pan%20American%20Energy%
Method	GET
Parameter	disputeId
Attack	577593) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20Ellen%20Baca%20v.%20United%20Mexican%20States%20(ICSID%20Case%2
Method	GET
Parameter	disputeId
Attack	513980) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20Howard%20Family%20Trust%20v.%20Government%20of%20Canada%20(PCA
Method	GET
Parameter	disputeId

Attack	708490) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20Co.%20KG%20(Sweden%20and%20Europe)%20v.%20The%20Federal%20Rep
Method	GET
Parameter	disputeId
Attack	664896) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20Trade%20S.A.%20v.%20Republic%20of%20Turkey%0D%0A(ICSID%20Case%
Method	GET
Parameter	disputeId
Attack	664352) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?H%20Enterprises%20Investments,%20Inc.%20v.%20Arab%20Republic%20of%20E
Method	GET
Parameter	disputeId
Attack	868291) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20Dominion%20Energy%20Holdings,%20L.P.%20v.%20Dominican%20Republic%
Method	GET
Parameter	disputeId
Attack	646367) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20Montenegro%20and%20Republic%20of%20Serbia%20(UNCITRAL)&ID=10&Lo
Method	GET
Parameter	disputeId
Attack	601349) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20Contracting,%20W.L.L.%20and%20Fouad%20Mohammed%20Thunyan%20Alg
Method	GET
Parameter	disputeId
Attack	1362931) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20Trading,%20Inc.%20v.%20Democratic%20Republic%20of%20the%20Congo%
Method	GET
Parameter	disputeId
Attack	642152) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20Dohme%20(I.A.)%20LLC%20v.%20Republic%20of%20Ecuador%20(PCA%20C
Method	GET
Parameter	disputeId
Attack	1259776) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20ARB(AF)/04/4)&ID=10&Location=Mexico%20-%20Gemplus,%20S.A.,%20SLP,%
Method	GET
Parameter	disputeId
Attack	1028277) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=India%20- %20Vodafone%20Group%20v.%20Republic%20of%20India%20%5BII%5D%20(UNCITRAL)&disputeId=1350412&goback=%252fdisputedirectory%252fDisputeDo
Method	GET
Parameter	disputeId
Attack	1350412) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDoc_AllDocList?Fsortdisp=docasc%20%20%20%20%20%23Directory&ID=10&doclist=IC%252f0249
Method	GET
Parameter	doclist
Attack	IC%2f0249%2f01') UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?%20ARB/03/30)&ID=10&Location=Argentina%20-%20Azurix%20Corp.%20v.%20Arg

Method	GET
Parameter	disputeId
Attack	556423) UNION ALL select NULL --
Evidence	All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists
Instances	31
Solution	Do not trust client side input, even if there is client side validation in place. In general, type check all data on the server side. If the application uses JDBC, use PreparedStatement or CallableStatement, with parameters passed by '?' If the application uses ASP, use ADO Command Objects with strong type checking and parameterized queries. If database Stored Procedures can be used, use them. Do *not* concatenate strings into queries in the stored procedure, or use 'exec', 'exec immediate', or equivalent functionality! Do not create dynamic SQL queries using simple string concatenation. Escape all data received from the client. Apply a 'whitelist' of allowed characters, or a 'blacklist' of disallowed characters in user input. Apply the principle of least privilege by using the least privileged database user possible. In particular, avoid using the 'sa' or 'db-owner' database users. This does not eliminate SQL injection, but minimizes its impact. Grant the minimum database access that is necessary for the application.
Other information	RDBMS [Microsoft SQL Server] likely, given UNION-specific error message regular expression [\QAll queries combined using a UNION, INTERSECT or EXCEPT opera The vulnerability was detected by manipulating the parameter with an SQL UNION clause to cause a database error message to be returned and recognised
Reference	https://www.owasp.org/index.php/Top_10_2010-A1 https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet
CWE Id	89
WASC Id	19
Source ID	1

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 opera
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat=&docid=845&id=201&subcat=%22%26timeout+%2FT+15%26%22&toc=content
Method	POST
Parameter	subcat
Attack	"&timeout /T 15&"
URL	http://dev.investorstatelawguide.com/documents/documents/AF-0001-26%20-%20ADF%20v.%20US%20-%20Canada%201128%20Submission.pdf%23navpanes
Method	GET
Parameter	query
Attack	query"|timeout /T 15
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1%7Ctimeout+%2FT+15&DocLanguage_Fren
Method	GET
Parameter	DocLanguage_English
Attack	1|timeout /T 15
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_Spanish=1&DocumentLanguage=S&ID=10&aprule=&aprule_arbrule_lcia_19
Method	GET
Parameter	doccat_21
Attack	1;start-sleep -s 15
URL	http://dev.investorstatelawguide.com/ResearchTools/DTSearchFTS? All_Arbitrator=&All_ArbitratorRules=&All_agreement_id=&All_circDate1=01%2F01%2F1899&All_circDate2=04%2F24%2F2019&All_filter_country_id=&DispId=c2%2C
Method	GET
Parameter	c10_param
Attack	";sleep 15;"
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_Spanish=1&DocumentLanguage=S&ID=10&aprule=&aprule_arbrule_lcia_19
Method	GET
Parameter	aprule_scc_arbrule_2007
Attack	1";start-sleep -s 15
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_G
Method	GET
Parameter	aprule_icsid_addfac_2003
Attack	1"&sleep 15&"
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?ID=10%27%3Bstart-sleep+-s+15&aprule=&aprule_arbrule_lcia_1998=1&aprule_icsid_addf
Method	GET

Parameter	ID
Attack	10';start-sleep -s 15
URL	http://dev.investorstatelawguide.com/documents/documents/AF-0001-05%20-%20ADF%20v.%20US%20-%20Minutes%20of%20First%20Session.pdf%23navpar
Method	GET
Parameter	query
Attack	query&timeout /T 15
URL	http://dev.investorstatelawguide.com/start-your-trial?City=ZAP%27%7Ctimeout+%2FT+15&Country=Albania&Email=ZAP&EnableEditProfile=1&Firm_Institution=ZAP
Method	GET
Parameter	City
Attack	ZAP'|timeout /T 15
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_G
Method	GET
Parameter	search
Attack	PJSC Ukrnafta v. Russian Federation, PCA Case No. 2015-34, Swiss Federal Supreme Court Order, 23 November 2017 [English Translation]&sleep 15&
URL	http://dev.investorstatelawguide.com/ResearchTools/JurisprudenceCitators?id=11%22%3Bstart-sleep+-s+15&toc=content&type=
Method	POST
Parameter	id
Attack	11";start-sleep -s 15
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_G
Method	GET
Parameter	doccat_3
Attack	1;sleep 15;
URL	http://dev.investorstatelawguide.com/ResearchTools/SubjectNavigator?ftypo=1&fuzziness=2&id=50%27%26sleep+15%26%27&search=ZAP&searchType=any&sten
Method	GET
Parameter	id
Attack	50'&sleep 15&'
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1%27%3Bstart-sleep+-s+15&DocLanguage_
Method	GET
Parameter	DocLanguage_English
Attack	1';start-sleep -s 15
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_G
Method	GET
Parameter	doccat_23
Attack	1"&sleep 15&"
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_G
Method	GET
Parameter	mainfilter
Attack	";sleep 15;"
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_G
Method	GET
Parameter	doccat_2
Attack	1';sleep 15;'
URL	http://dev.investorstatelawguide.com/User/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLangua
Method	GET
Parameter	DocLanguage_German
Attack	1'&sleep 15&'
URL	http://dev.investorstatelawguide.com/start-your-trial?query=query%26timeout+%2FT+15
Method	POST
Parameter	query
Attack	query&timeout /T 15
Instances	142
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 v OS-level examples include the Unix chroot jail, AppArmor, and SELinux. In general, managed code may provide some protection. For example, java.io.FilePermission 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 application 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 pron

	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 a 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 If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant qu 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 st 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 When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra inpu 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 inc Note that proper output encoding, escaping, and quoting is the most effective solution for preventing OS command injection, although input validation may provide s 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 att
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)	**Cross Site Scripting (Reflected)**
Description	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard When an attacker gets a user's browser to execute his/her code, the code will run within the security context (or zone) of the hosting web site. With this level of privile There are three types of Cross-site Scripting attacks: non-persistent, persistent and DOM-based. Non-persistent attacks and DOM-based attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containin Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time. Examples of an attacker's favorite targets often inc
URL	http://dev.investorstatelawguide.com/ResearchTools/DTSearchFTS?All_Arbitrator=&All_ArbitratorRules=&All_agreement_id=&All_circDate1=%22+onMouseOver%3D%22alert%281%29%3B&All_circDate2=&All_filter_country_id=&Disp
Method	GET
Parameter	All_circDate1
Attack	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_G
Method	GET
Parameter	toc
Attack	</script><script>alert(1);</script><script>
Evidence	</script><script>alert(1);</script><script>
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_Spanish=1&DocumentLanguage=S&ID=10&aprule=&aprule_arbrule_lcia_19
Method	GET
Parameter	refresh
Attack	"><script>alert(1);</script>
Evidence	"><script>alert(1);</script>
URL	http://dev.investorstatelawguide.com/User/Welcome/TermsPhrases?letter=x&searchType=javascript%3Aalert%281%29%3B&toc=termsPhrases
Method	POST
Parameter	searchType
Attack	javascript:alert(1);
Evidence	javascript:alert(1);
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_English=1&DocumentLanguage=%22%3E%3Cscript%3Ealert%281%29%3
Method	GET
Parameter	DocumentLanguage
Attack	"><script>alert(1);</script>
Evidence	"><script>alert(1);</script>
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?id=%3C%2Fscript%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3Cscript
Method	GET
Parameter	id
Attack	</script><script>alert(1);</script><script>
Evidence	</script><script>alert(1);</script><script>
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_G
Method	GET
Parameter	treatycat
Attack	"><script>alert(1);</script>
Evidence	"><script>alert(1);</script>
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?Global=Yes&cat=&id=201&search_title=ZAP&subcat=%22%3E%3Cscript%3Ealert%281%29%3

Method	GET
Parameter	subcat
Attack	"><script>alert(1);</script>
Evidence	"><script>alert(1);</script>
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?PageNumber=1&id=10&toc=%3C%2Fscript%3E%3Cscript%3Ealert%281%29%3B%3C%
Method	GET
Parameter	toc
Attack	</script><script>alert(1);</script><script>
Evidence	</script><script>alert(1);</script><script>
URL	http://dev.investorstatelawguide.com/ResearchTools/JurisprudenceCitators?id=11&type=%3C%2Ftd%3E%3Cscript%3Ealert%281%29%3B%3C%2Fscript%3E%3
Method	GET
Parameter	type
Attack	</td><script>alert(1);</script><td>
Evidence	</td><script>alert(1);</script><td>
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_G
Method	GET
Parameter	refresh
Attack	"><script>alert(1);</script>
Evidence	"><script>alert(1);</script>
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_Spanish=1&DocumentLanguage=%22%3E%3Cscript%3Ealert%281%29%
Method	GET
Parameter	DocumentLanguage
Attack	"><script>alert(1);</script>
Evidence	"><script>alert(1);</script>
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_English=1&DocumentLanguage=E&ID=10&aprule=&aprule_arbrule_lcia_199
Method	GET
Parameter	refresh
Attack	"><script>alert(1);</script>
Evidence	"><script>alert(1);</script>
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_English=1&DocumentLanguage=E&ID=%3C%2Fscript%3E%3Cscript%3Ea
Method	GET
Parameter	ID
Attack	</script><script>alert(1);</script><script>
Evidence	</script><script>alert(1);</script><script>
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_G
Method	GET
Parameter	aprule
Attack	" onMouseOver="alert(1);
Evidence	" onMouseOver="alert(1);
URL	http://dev.investorstatelawguide.com/Home/UserSession
Method	POST
Parameter	HiddenSelectedValue
Attack	"><script>alert(1);</script>
Evidence	"><script>alert(1);</script>
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_English=1&DocumentLanguage=E&ID=10&aprule=%22%3E%3Cscript%3E
Method	GET
Parameter	aprule
Attack	"><script>alert(1);</script>
Evidence	"><script>alert(1);</script>
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_G
Method	GET
Parameter	DocumentLanguage
Attack	"><script>alert(1);</script>
Evidence	"><script>alert(1);</script>
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_English=1&DocumentLanguage=E&ID=10&aprule=&aprule_arbrule_lcia_199
Method	GET
Parameter	treatycat
Attack	"><script>alert(1);</script>
Evidence	"><script>alert(1);</script>

URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_G
Method	GET
Parameter	index
Attack	</script><script>alert(1);</script><script>
Evidence	</script><script>alert(1);</script><script>
Instances	104
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. Examples of libraries and frameworks that make it easier to generate properly encoded output include Microsoft's Anti-XSS library, the OWASP ESAPI Encoding moc Phases: Implementation; Architecture and Design Understand the context in which your data will be used and the encoding that will be expected. This is especially important when transmitting data between different For any data that will be output to another web page, especially any data that was received from external inputs, use the appropriate encoding on all non-alphanume Consult the XSS Prevention Cheat Sheet for more details on the types of encoding and escaping that are needed. Phase: Architecture and Design For any security checks that are performed on the client side, ensure that these checks are duplicated on the server side, in order to avoid CWE-602. Attackers can b If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant qu Phase: Implementation For every web page that is generated, use and specify a character encoding such as ISO-8859-1 or UTF-8. When an encoding is not specified, the web browser may To help mitigate XSS attacks against the user's session cookie, set the session cookie to be HttpOnly. In browsers that support the HttpOnly feature (such as more re 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 When performing input validation, consider all potentially relevant properties, including length, type of input, the full range of acceptable values, missing or extra input Ensure that you perform input validation at well-defined interfaces within the application. This will help protect the application even if a component is reused or move
Reference	http://projects.webappsec.org/Cross-Site-Scripting http://cwe.mitre.org/data/definitions/79.html
CWE Id	79
WASC Id	8
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 informati
URL	http://dev.investorstatelawguide.com/Treaties/Index?cat&search=ZAP&sort=A&tab&toc=mainAnnot
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/Treaties/AnnotDocument?agreementID=286&cat&tabcontent=yes&toc=annotSection
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/Treaties/index?cat=nafta&toc=mainAnnot
Method	GET
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
URL	http://dev.investorstatelawguide.com/Treaties/Index?cat&tab&toc=mainAnnot
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/Home/Register?Length=0
Method	POST
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/Treaties/index?cat=regsec&toc=mainAnnot
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/Treaties/images/icon-search2.gif%5C%22
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/Treaties/index?cat=bit&toc=mainAnnot
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error

URL	http://dev.investorstatelawguide.com/Treaties/index?cat=intlaw&toc=mainAnnot
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/DTSearchFTS?All_Arbitrator&All_ArbitratorRules&All_agreement_id&All_circDate1=01%2F01%2F1899&All_circDa
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/Treaties/index?cat=fta&toc=mainAnnot
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/Treaties/index?cat=bit%7Cfta%7Cnafta%7Cother%7Cregsec&toc=mainAnnot
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/Treaties/index?cat=other&toc=mainAnnot
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/Treaties/index?cat&toc=mainAnnot
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/Treaties/index?cat=arbrules&toc=mainAnnot
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
URL	http://dev.investorstatelawguide.com/ResearchTools/DTSearchFTS? All_Arbitrator&All_ArbitratorRules&All_agreement_id&All_circDate1&All_circDate2&All_filter_country_id&DispId=test&InvestmentTreaty_CountryId&InvestmentTreaty_Tre
Method	GET
Evidence	HTTP/1.1 500 Internal Server Error
Instances	17
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 (b
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/ResearchTools/SubjectNavigator? ci=52501%2352501&id=50&kwList=37858%2C37819%2C37820%2C41891%2C52501&search=Clayton%2FBilcon+v.+Canada&toc=ZAP+%251%21s%252%21s%
Method	GET
Parameter	toc
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/ResearchTools/SubjectNavigator?id=50&tab=r&toc=content
Method	POST
Parameter	stem
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	http://dev.investorstatelawguide.com/ResearchTools/SubjectNavigator?id=50&tab=r&toc=content
Method	POST
Parameter	thes
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	http://dev.investorstatelawguide.com/ResearchTools/PublicationCitators?id=264
Method	POST
Parameter	search_title
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat=arbitrationrules&id=201&subcat&toc=content
Method	POST
Parameter	search_title
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat=ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n
Method	POST
Parameter	cat
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat&docid=845&id=201&subcat&toc=content

Method	POST
Parameter	search_title
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat=arbitrationrules&id=201&subcat=ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%2
Method	POST
Parameter	subcat
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat=ZAP%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n%25s%25n
Method	POST
Parameter	cat
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	http://dev.investorstatelawguide.com/ResearchTools/JurisprudenceCitators?id=11&toc=content&type
Method	POST
Parameter	search_title
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
URL	http://dev.investorstatelawguide.com/ResearchTools/SubjectNavigator?id=50&tab=r&toc=content
Method	POST
Parameter	searchType
Attack	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
Instances	11
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)	**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/
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	1
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)	**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/
Method	GET
Parameter	Cache-Control
Evidence	private
Instances	1
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)	**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/
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. 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	https://dev.investorstatelawguide.com/
Method	GET
Parameter	X-XSS-Protection
Instances	1
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)	**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 legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat=investmenttreaty&docid=1550&id=201&subcat=bit&toc=content
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat&docidclose=1560&id=201&subcat&toc=content
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/ResearchTools/SubjectNavigator?ci=53707&exList&id=50&kwList=26229,53707,&search&searchBranchLevel&toc=content
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/ResearchTools/SubjectNavigator?ci=21099&exList&id=50&kwList=27200,21099,&search&searchBranchLevel&toc=content
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=El%20Salvador%20-%20Pac%20Rim%20Cayman%20LLC.%20v.%20Republic%20of%20El%20Salvador%20(ICSID%20Case%20No.%20ARB/09/12)&disputeId=744863&goback=%2
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/ResearchTools/JurisprudenceCitators?cidsp=740749&disputeID=740749&id=11&sort&type=gatt
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Panama%20-%20Retire%20in%20Chiriqui,%20S.A.%20and%20others%20v.%20Republic%20of%20Panama&disputeId=924699&goback=%252fdisputedirectory%252fDispute
Method	GET
Parameter	X-Content-Type-Options

URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Guatemala%20-%20TECO%20Guatemala%20Holdings,%20LLC%20v.%20Republic%20of%20Guatemala%20(ICSID%20Case%20No.%20ARB/10/23)&disputeId=1028290&goba
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/ResearchTools/JurisprudenceCitators?cidsp=555927&disputeID=555927&id=11&sort&type=gatt
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Guatemala%20-%20TECO%20Guatemala%20Holdings,%20LLC%20v.%20Republic%20of%20Guatemala%20(ICSID%20Case%20No.%20ARB/10/23)&disputeId=1028290&goba
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat&docid=3933&id=201&subcat&toc=content
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Spain%20-%20Mathias%20Kruck%20and%20others%20v.%20Kingdom%20of%20Spain%20(ICSID%20Case%20No.%20ARB/15/23)&disputeId=1426125&goback=%252fd
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat=investmenttreaty&docid=4328&id=201&subcat=bit&toc=content
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/documents/documents/IC-0041-01_EDF.pdf
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Kyrgyz%20Republic%20-%20Lee%20Jong%20Baek%20and%20Central%20Asian%20Development%20Corporation%20v.%20Kyrgyz%20Republic&disputeId=1032233&goback=%252fdis
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Slovak%20Republic%20-%20European%20American%20Investme 17)&disputeId=1118279&goback=%252fdisputedirectory%252fDisputeDocument%253fPageNumber%253d83%2526id%253d10%2526toc%253ddisputedirectory&
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/ResearchTools/SubjectNavigator?ci=33428&exList&id=50&kwList=26229,33428,&search&searchBranchLevel&toc=content
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/ResearchTools/SubjectNavigator?ci=39175&exList&expandWholeBranchList=39175&id=50&kwList=25889,39175,&search&sea
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/Treaties/AnnotDocument?agreementID=465&cat&tabcontent=yes&toc=annotSection
Method	GET
Parameter	X-Content-Type-Options
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Romania%20-%20Gabriel%20Resources%20Ltd.%20and%20Gabriel%20Resources%20(Jersey)%20v.%20Romania%20(ICSID%20Case%20No.%20ARB/15/31)&disputeId=125
Method	GET
Parameter	X-Content-Type-Options
Instances	11208
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
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 browse 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)	**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/documents/documents/IC-0018-06%20Siemens.pdf%23navpanes=0&Page=1
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/disputedirectory/DisputeDocument?PageNumber=62&id=10&sorttab=scd_asc&toc=disputedirectory
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/documents/documents/UN-0122-03%20-%20Everest%20Estate%20v.%20Russia%20-%20PCA%20Press%20Release%20II.pdf%23navpanes=0&Page=1
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/ResearchTools/SubjectNavigator?ci=26786&exList&id=50&kwList=26562,26786,&search&searchBranchLevel&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/ResearchTools/ArticleCitator?cat=investmenttreaty&docid=1866&id=201&subcat=bit&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/documents/documents/UN-0012-29%20-%20Thunderbird%20v.%20Mexico%20-%20Resp%20Rejoinder%20PO9.pdf%23navpanes=0&Page=1
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/ResearchTools/ArticleCitator?AgreementID=110&ProvCode=Art52.(2)&aaprovid=51865&cat&docid=809&id=201&sort&subcat&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/ResearchTools/SubjectNavigator?ci=38249&exList&id=50&kwList=27130,38249,&search&searchBranchLevel&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/documents/documents/New%20York%20Convention.pdf%23navpanes=0&Page=1
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/ResearchTools/ArticleCitator?AgreementID=125&ProvCode=Rule40.(3)&aaprovid=55518&cat&docid=828&id=201&sort&subcat&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/disputedirectory/DisputeDocument?PageNumber=16&id=10&toc=disputedirectory
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/documents/documents/UN-0004-07%20Chevron%20I%20Judgment%20of%20Hague%20Court.pdf%23navpanes=0&Page=1
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/ResearchTools/ArticleCitator?cat&docid=98&id=201&subcat&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/ResearchTools/ArticleCitator?cat&docid=4888&id=201&subcat&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/ResearchTools/ArticleCitator?AgreementID=114&ProvCode=Rule34&aaprovid=57182&cat&docid=855&id=201&sort&subcat&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/ResearchTools/SubjectNavigator?ci=39324&exList&expandWholeBranchList=39324&id=50&kwList=37858,39324,&search&searchBranchLevel&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/documents/documents/Non-Investment%20Treaty%20Doc.pdf%23navpanes=0&Page=1
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/ResearchTools/FullTextSearch?id=97&selNodeId=27126&tab=r&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/ResearchTools/ArticleCitator?AgreementID=169&ProvCode=Art58&aaprovid=58195&cat&docid=880&id=201&sort&subcat&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/ResearchTools/FullTextSearch?id=97&selNodeId=51150&tab=r&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>
Instances	11352
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	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Czech%20Republic%20-%20European%20Media%20Ventures%2
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Venezuela%20-%20Venezuela%20Holdings%20B.V.%20and%20ot
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat&docidclose=880&id=201&subcat&toc=content
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Slovak%20Republic%20-%20European%20American%20Investme
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/ResearchTools/SubjectNavigator?ci=38430&exList&expandWholeBranchList=38430&id=50&kwList=37710,38430,&search&sea
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument?PageNumber=67&id=10&sorttab=scd_asc&toc=disputedirectory
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/documents/documents/IC-0281-04%20-%20Rios%20v.%20Chile%20-%20Respondent%20Memorial%5BSpanish%5D.pdf%
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Egypt%20-%20Malicorp%20Limited%20v.%20Arab%20Republic%
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Croatia%20-%20MOL%20Hungarian%20Oil%20and%20Gas%20C
Method	GET
Parameter	X-XSS-Protection

URL	http://dev.investorstatelawguide.com/documents/documents/UN-0043-02%20-%20Nordzucker%20v.%20Poland%20-%20Second%20Partial%20Award.pdf%23na
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Canada%20-%20Crompton%20(Chemtura)%20Corporation%20v.%
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat=investmenttreaty&docid=6946&id=201&subcat=bit&toc=content
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/documents/documents/OT-0001-02%20-%20France%20Telecom%20v.%20Lebanon%20-%20Decision%20I.pdf%23navpane
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Senegal%20-%20Soci%C3%A9t%C3%A9%20Ouest%20Africaine
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/documents/documents/FTA-0039%20-%20Oman-United%20States%20Free%20Trade%20Agreement%20(2006)%20(excerp
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDocument? DocLanguage_All=1&DocLanguage_English=1&DocLanguage_French=1&DocLanguage_German=1&DocLanguage_Spanish=1&DocLanguage_other=1&DocumentLa
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/DisputeDirectory/DisputeDoc_AllDocList?ID=10&Location=Venezuela%20-%20Vannessa%20Ventures%20Ltd.%20v.%20Boliv
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/documents/documents/AF-0001-27%20-%20ADF%20v.%20US%20-%20Mexico%201128%20Submission.pdf%23navpanes
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/ResearchTools/ArticleCitator?cat=investmenttreaty&docid=4463&id=201&subcat=bit&toc=content
Method	GET
Parameter	X-XSS-Protection
URL	http://dev.investorstatelawguide.com/disputedirectory/DisputeDoc_AllDocList?ID=10&doclist=IC%2f0052%2f02&goback=%2fdisputedirectory%2fDisputeDocument
Method	GET
Parameter	X-XSS-Protection
Instances	15741
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 a 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 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/ResearchTools/SubjectNavigator?id=50&tab=r&toc=content
Method	GET
Parameter	UserCIS
Evidence	Set-Cookie: UserCIS
URL	http://dev.investorstatelawguide.com/notepad-login
Method	POST
Parameter	RePassword

Evidence	Set-Cookie: RePassword
URL	http://dev.investorstatelawguide.com/notepad-login
Method	POST
Parameter	UserId
Evidence	Set-Cookie: UserId
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
URL	http://dev.investorstatelawguide.com/notepad-login
Method	POST
Parameter	ReUserId
Evidence	Set-Cookie: ReUserId
URL	http://dev.investorstatelawguide.com/notepad-login
Method	POST
Parameter	Password
Evidence	Set-Cookie: Password
Instances	7
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